National Security Agency
Cybersecurity Technical Report

Recommendations for Configuring Adobe Acrobat Reader DC in a Windows Environment

JAN 2022

U/OO/104771-22
PP-22-0042
Version 2.0

Notices and history

Document change history

Date	Version	Description
December 2015	1.0	Initial Release
January 2022	2.0	Revised Version

Disclaimer of warranties and endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Trademark recognition

Adobe Acrobat, Reader, and Adobe PDF are registered trademarks of Adobe Systems Incorporated. ▪ Microsoft, Windows, Outlook, Office, and SharePoint are registered trademarks of Microsoft Corporation.

Publication information

Author(s)

National Security Agency
Cybersecurity Directorate
Endpoint Security

Contact information

Client Requirements / General Cybersecurity Inquiries:
Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov

Media inquiries / Press Desk:
Media Relations, 443-634-0721, MediaRelations@nsa.gov

Defense Industrial Base Inquiries / Cybersecurity Services:
DIB Cybersecurity Program, DIB_Defense@cyber.nsa.gov

Purpose

This document was developed in furtherance of NSA's cybersecurity missions. This includes its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense information systems, and the Defense Industrial Base, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Executive summary

Malicious cyber actors have a long and well-documented history of targeting users (including Department of Defense and National Security Systems) using malicious Portable Document Files (PDFs). However, modern security features for sandboxing and access control can help constrain what malicious PDFs can do, and can be rolled out en masse, limiting this common access vector at scale.

This configuration guide provides recommendations on configuring Adobe Acrobat® Reader® DC in a Windows® environment. Administrators operating in a typical environment where Acrobat Reader is used solely for viewing PDF documents may use the Appendix: Configuring Settings for Adobe's Acrobat Reader DC as a quick guide to configure the Adobe Customization Wizard with the recommendations suited to their environment.

The recommendations flagged in the Appendix as "always" are sufficient for most environments and are suitable for security compliance checklists. In some situations, however, users may utilize features of Adobe's Acrobat Reader requiring scripting or data sharing. In these cases, administrators should carefully review this configuration guide to select configuration options that will have minimal impact on usability while providing the most protection.

All administrators should understand the implications of the new cloud features and review Section 3.4: Document Cloud interaction for guidelines on configuring them or disabling them as required for the environment.

Contents

Figures

Tables

1. Introduction

The greatest threat to users of Adobe's Acrobat Reader is opening a PDF file that contains malicious executable content (hereafter referred to as "malicious documents"). The risk of a user receiving such a document through email or web surfing is high. Phishing attacks frequently include malicious PDF attachments or links to download malicious PDFs.

Adobe's Acrobat Reader DC (herein "Reader") can run in a sandboxed process to help protect the user from malicious documents. Acrobat Reader DC is the latest version and replaces Acrobat Reader XI. The "DC" in the title stands for "Document Cloud," which refers to the cloud-based features introduced in Acrobat Reader DC. This configuration guide presents NSA-recommended configuration settings for Reader that allow system administrators to minimize the risk of executable content and other malicious activity in a Windows environment.

Administrators can configure Reader to minimize the risk of malicious activity.

Reader settings fall into two broad types: those that should be used in all environments and those for environments with unique security requirements.

Section 2 describes the settings applicable to all environments, such as settings for sandboxing features like Protected Mode, Protected View, and AppContainer.

Section 3 describes settings that should be tailored to the specific security needs of the environment.

Section 4 includes information for using Adobe's Customization Wizard to configure the necessary settings for uniform distribution of the software throughout an enterprise or on a standalone system.

Section 5 includes information about patching and upgrading. When upgrading Reader, previous versions need to be removed.

The Appendix: Configuring Settings for Adobe's Acrobat Reader DC lists all of the Reader security-related settings with recommendations for the environments that should configure those settings. Reader's digital signature capabilities, digital rights management, and other related security settings are beyond the scope of this configuration guide.

Simply configuring Acrobat's security settings is **not** enough to completely secure a system. As with all commercial products, the system administrator must also configure a secure operating environment and stay current with all security-related patches and updates to that environment.

2. Environment-agnostic settings

The following settings are applicable to all environments. Adjustments to these settings should have minimal impact to workflow and productivity yet provide some protections against malicious executable content.

2.1. The sandbox

Beginning with version X, Acrobat Reader includes sandboxing technology to constrain the access that JavaScript and other executable content has to a system's resources. Reader currently includes three sandboxing capabilities: ***Protected Mode***, ***Protected View***, and ***AppContainer***.

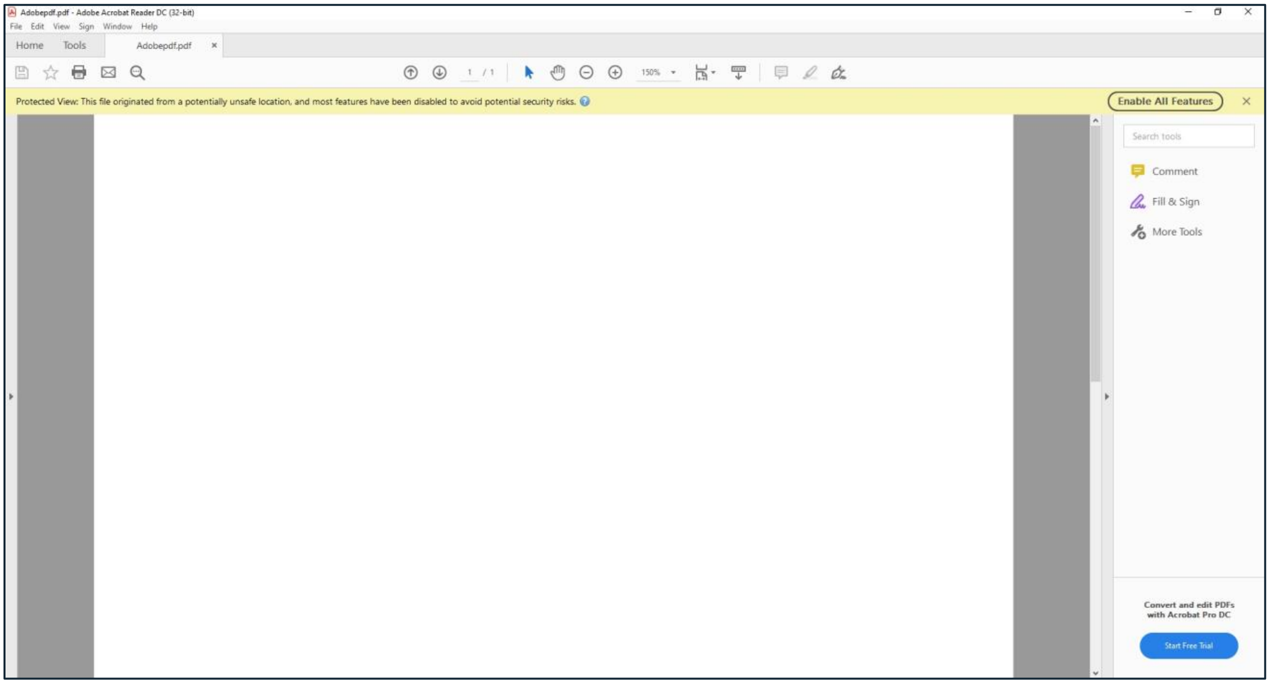
2.1.1. Protected Mode

Protected Mode was specifically developed for Windows environments and, when enabled, Reader opens the PDF document with the executable content (e.g., JavaScript) enabled, but within a sandbox that restricts the document's execution and access through operating system security controls. For example, a process inside the sandbox cannot access processes outside the sandbox without going through a trusted broker process. The sandbox restricts access to system resources, such as the file system and the registry. The execution appears seamless to the user who can still take advantage of the functionality of the executable content as long as the executable content behaves within certain limits.

Prior to the existence of the Protected Mode sandbox, the typical security practice was to disable all JavaScript to prevent execution of malicious scripts. Protected Mode differs from disabling JavaScript because the document is opened in a sandboxed state instead. The constrained execution environment limits all actions, not just those within scripts, and can deny most malicious activity.

2.1.2. Protected View

Protected View, available since Adobe Reader XI, is a more restrictive sandbox than Protected Mode and it is only available when Protected Mode is enabled. When Protected View is enabled, Acrobat opens the PDF document in the Protected Mode sandbox, but with executable content and scripts disabled. The user can still view the document and will see a yellow message bar across the top with a warning that some features of the document have been disabled, as shown here:



Adobepdf.pdf - Adobe Acrobat Reader DC (32-bit)
File Edit View Sign Window Help
Home Tools Adobepdf.pdf ×
1 / 1
150%
Enable All Features
Search tools
Comment
Fill & Sign
More Tools
Convert and edit PDFs with Acrobat Pro DC
Start Free Trial

Protected View: This file originated from a potentially unsafe location, and most features have been disabled to avoid potential security risks.

Figure 1: The Protected View yellow message bar[1]

The user has the option to enable those features after deciding whether to trust the document and whether those features are necessary. Even if the user decides to trust the document, the PDF will still be opened in the Protected Mode sandbox.

Protected View is essential to prevent users from inadvertently opening and executing malicious active content. Allowing the user to view the document prior to enabling active content can prevent many phishing and other attacks. Once the user views the

[1] Adobe product screenshot(s) reprinted with permission from Adobe.

document and enables the content, Reader adds the document as a privileged location (see next section) for that user and bypasses protected view on subsequent openings of that document. Note that disabling “*TrustedFolders*” will prevent users from trusting documents, which would prevent them from using the “Enable All Features” button in protected view (see section 2.3: Privileged Locations for more information.

2.1.3. AppContainer

AppContainer is an application-level sandbox provided by Microsoft® Windows® and, like Protected Mode and Protected View, it blocks application processes from reading and writing to files outside of its boundaries. AppContainer is supported on all distributions and requires that Protected Mode be enabled.

2.2. Enhanced security and FeatureLockDown

The enhanced security setting enforces some essential security elements that help to protect users. According to Adobe’s documentation, enhanced security “hardens” applications against risky actions by doing the following for any document not specifically trusted [1]:

- Prevents access across DNS domains: externally requested content must adhere to a “same-origin” policy. Without a server-based cross-domain policy file, that content is blocked.
- Prohibits script and data injection via a Fast Data Finder (FDF), XML Forms Data Format (XFDF), and XML Data Package (XDP) when not returned as the result of a POST from the PDF. These data formats are commonly used when submitting forms.
- Blocks stream access to XObjects that can include external content like images and fonts.
- Stops silent printing to a file or hardware printer.

Under the HKEY_LOCAL_MACHINE (HKLM) hive, Reader includes a registry key called *FeatureLockDown*, which allows administrators to configure certain security settings. Values under *FeatureLockDown* do not necessarily disable functionality. The purpose of *FeatureLockDown* is to roll out security settings at scale and prevent users from changing settings through the Reader GUI. Some of the same settings are also under HKEY_CURRENT_USER (HKCU), but configuring those under HKCU alone is not recommended because HKCU is writeable by the user.

Enhanced security and Protected Mode are turned on by default in Reader, but they are not locked, meaning a user can disable them through the GUI. Protected View and AppContainer are not turned on by default and require Protected Mode to be enabled. All four should be enabled and locked down to prevent the end-user from disabling them. This should have minimal impact to productivity and workflow, and if necessary, the administrator can set privileged locations for exceptions (see section 2.3: Privileged Locations).

Table I: Configuring enhanced security, Protected Mode, Protected View, and AppContainer

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
bEnhancedSecurityStandalone	REG_DWORD	Set to 1
bEnhancedSecurityInBrowser	REG_DWORD	Set to 1
bProtectedMode	REG_DWORD	Set to 1
iProtectedView	REG_DWORD	Set to 2
bEnableProtectedModeAppContainer	REG_DWORD	Set to 1

HKCU\Software\Adobe\Acrobat Reader\DC\TrustManager		
bEnableAlwaysOutlookAttachmentProtectedView	REG_DWORD	Set to 0

The setting *bEnableAlwaysOutlookAttachmentProtectedView* from Table II: Configuring enhanced security, Protected Mode, Protected View, and AppContainer only takes effect for attachments received from Microsoft Outlook® in Office® 2010 and later. Previous versions of Outlook do not append origin information to attachments.

2.3. Privileged locations

Privileged locations allow the user to selectively trust files, folders, and sites to bypass some security restrictions such as enhanced security and Protected View. By default, the user can create privileged locations through the GUI using the Preferences dialog (*Edit → Preferences → Security (Enhanced)*). Alternately, a file is automatically added to the privileged files when the user clicks the “Enable All Features” button in the warning banner while in Protected View in that file. The administrator can disable the user’s ability to create privileged sites through the Preferences dialog by using the settings in Table IV: Locking privileged locations.

Disabling the GUI options to create privileged hosts and enabling Protected Mode, Protected View, AppContainer, and enhanced security as described in Table III: Configuring enhanced security, Protected Mode, Protected View, and AppContainer above will result in the user needing to first view all documents with active content disabled and to take explicit action to enable active content.

Table IV: Locking privileged locations

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
bDisableTrustedSites	REG_DWORD	Set to 1

Administrators can prevent a user from trusting files and folders with the *bDisableTrustedFolders* registry key (see Table IV). However, in doing so, they will prevent users from transitioning out of Protected View, which will prevent embedded scripts from executing, reducing PDF usability.

The settings in Table V: Locking privileged locations prevent the user from directly adding sites as privileged locations through the GUI. This will have a minimal impact on workflow since the user can still enable active content after opening a file (through the yellow message bar), and Reader will create a privileged location for only that file. If workflow is impacted, the administrator can create privileged sites as needed for the user (refer to the Acrobat Application Security Guide [1]). The administrator can also add trusted sites in Internet Explorer or Edge as privileged locations, or can allow the user to add trusted sites to preemptively trust documents. To do this for either browser follow these steps: (Open *Control Panel* → *Internet Options* → *Security* → *Trusted Sites* → *Sites* → <site to add>)

2.4. Attachments

In addition to malicious scripts, PDF documents can have attachments, which may also contain malicious content and present a security risk. The administrator can disable the user's ability to access attachments with the setting in Table VI: Disabling attachmentsTable .

Table VII: Disabling attachments

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
iFileAttachmentPerms	REG_DWORD	Set to 0

This setting locks out the user's ability to configure the PDF File Attachment setting in the Trust Manager (*Edit* → *Preferences* → *Trust Manager*, checkbox under PDF File Attachments) and disables opening or saving file attachments. This setting overrides any attachment deny list or allow list. Many environments do not have a requirement for PDF documents to contain attachments. However, in environments where users need collaborative document sharing capabilities via Reader, this setting would interrupt workflows.

A less restrictive but manageable approach is to set *iFileAttachmentPerms* to `0` and to allow only certain types of attachments. Reader allows the administrator to deny/allow specific attachment types and to automatically deny unlisted types. When using a deny list/allow list mechanism, the recommended approach is to block everything and allow only approved exceptions. To do this in Reader, disable unlisted attachment types with *iUnlistedAttachmentTypePerm* and then enable only those that are safe or needed with *tBuiltInPermList*. Table VIII: shows the necessary settings.

Table VIII: Adding attachment types to the allow list

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
iFileAttachmentPerms	REG_DWORD	Set to 0

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\ cDefaultLaunchAttachmentPerms		
iUnlistedAttachmentTypePerm	REG_DWORD	Set to 3
tBuiltInPermList	REG_SZ	Version:1|<extension>:<0-3>|…

For example, to allow *.docx* files and block *.exe* files the administrator would set *tBuiltInPermList* to the string *Version:1*|*.docx:2*|*.exe:3*| *etc*. The user will not be allowed to launch any .exe files and will be prompted for *.docx* files and given a choice to allow just that file, enable that extension always, or disable that extension always. As long as *iUnlistedAttachmentTypePerm* is set to `3`, any attachment type not listed in *tBuiltInPermList* will not launch.

Reader is installed with a default list of extensions that an administrator can customize in the registry or the Adobe Customization Wizard. The default list blocks common executable content, such as *.exe* and *.bat* files.

3. Tailored settings

Because the following settings can impact workflow and productivity, adjustments to them should be tailored to the specific security needs of the environment. Administrators that need to configure these specialized settings in order to preemptively trust or control certain documents should consult the most recent Adobe guidance for those settings.

3.1. Internet access from a document via hyperlink

PDF documents can contain hyperlinks to files or web sites that could lead a user to malicious content. By default, Reader cannot open hyperlinks in documents, but the user can change these settings through the GUI (*Edit → Preferences → Trust Manager*, button labeled "Change Settings" in the Internet Access section). The user can allow PDF files to access all web sites, block all access to websites, or create a custom list of websites to allow or block. The administrator can prevent the user from changing settings created by the administrator by using the *FeatureLockDown* key as in Table IX: Restricting hyperlinks, and, if desired, can block all access to hyperlinks from within a document.

Table X: Restricting hyperlinks

HKCU\Software\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms		
iURLPerms	REG_DWORD	Set to 1
tBuiltInPermList	REG_SZ	version:1|<site>:<1-3>|... (1 is always ask; 2 is always allow, 3 is always block)

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms		
iUnknownURLPerms	REG_DWORD	Set to 3 (block all unlisted sites)

NSA recommends to set *iURLPerms* to `1` which will prevent the user from following hyperlinks within a PDF document. In some cases, when it is desirable to allow a known set of trusted URLs, the *iURLPerms* key can be removed after *iUnknownURLPerms* is set to `3` and *tHostPerms* is set to a list of trusted URLs.

3.2. JavaScript

JavaScript extends the functionality of PDF documents, allowing for decision-driven content that greatly enhances the user experience. JavaScript is commonly used in electronic forms for recipients to complete, sign, and return documents electronically. Because JavaScript usage in PDFs is becoming more frequent, NSA recommends that administrators **not** change the default setting for Reader that allows JavaScript. Protected Mode and Enhanced security, as previously described, will help mitigate some of the security concerns due to allowing JavaScript within PDFs.

Historically, JavaScript has been a frequent attack vector. Therefore, some administrators may opt for a more secure environment at the cost of usability. For such environments where JavaScript must be disabled, the recommended configuration is to:

- Set Protected Mode, Protected View, AppContainer, and Enhanced Security as Table XI: Configuring enhanced security, Protected Mode, Protected View, and AppContainer suggests,
- Lock the privileged location settings as suggested in Table XII: Locking privileged locations, and
- Disable JavaScript and establish trusted locations for particular documents or locations where JavaScript is required for usability as shown in Table XIII: Disabling JavaScript and enabling trusted locations.

With this configuration, the user will not be able to execute JavaScript in any PDF file outside of trusted locations and will not be able to change the setting through the Reader GUI. The administrator can add particular files, directories, drives, or hosts as trusted locations that will bypass the JavaScript restrictions. This approach gives the administrator the ability to allow JavaScript functionality for particular files or locations, but greatly restricts the user's ability to exempt documents with JavaScript from the security mechanisms.

Table XIV: Disabling JavaScript and enabling trusted locations

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
bDisableJavaScript	REG_DWORD	Set to 1

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\<cTrustedFolders or cTrustedSites>\cAlwaysTrustedForJavaScript		
<tid> (such as t43 or t#)	REG_SZ	Valid path to a file, directory or host

In an environment where the user needs access to many documents that contain JavaScript, the administrator may spend significant time updating the trusted locations. There is always a tradeoff between risk and functionality, and sometimes the most secure settings prevent necessary functionality.

An administrator has an even more granular level of control with the ability to create allow lists and deny lists for particular JavaScript APIs. Generally, this requires significant administrative investment and is not a scalable or manageable solution. It is practical only for installations where there is a specific need for this level of granularity beyond the basic recommendations (refer to the Acrobat Application Security Guide for more information on using this feature).

3.3. Internet access from the Reader application

Reader includes features to enable access to online services such as Adobe.com, Office 365®, SharePoint®, and webmail. Administrators in some environments may need to disable the user's ability to store or access documents in external environments or to use external applications such as webmail. Most of this capability can be blocked by using the settings in Table XV: Disabling online service access. These settings should be tailored for individual environments since they will block useful features of Reader.

Reader allows the user to configure a webmail or Outlook account to send an open PDF document as an attachment. Outlook must be configured by the administrator on the local machine. If Outlook is not configured, the user cannot use it from within Reader. Webmail access would allow the user to bypass the need for Outlook and go to a webmail solution.

Some installations will need to block access to webmail. NSA recommends that administrators configure Reader to use Outlook and to block webmail functionality. Doing this will prevent users from inadvertently sending documents via non-official servers. If there is a requirement that users have access to the webmail feature in Reader, administrators should ensure that users are trained to use only official or accredited webmail servers.

Table XVI: Disabling online service access

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cSharePoint		
bDisableSharePointFeatures	REG_DWORD	Set to 1 (also disables Office 365)

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cCloud		
bDisableADCFileStore	REG_DWORD	Set to 1

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cWebmailProfiles		
bDisableWebmail	REG_DWORD	Set to 1

Currently, Reader requires the system administrator to apply updates; users cannot update Reader and do not need to see the update notifications. Disabling the automatic update feature for users will prevent Reader from prompting users but will not impact updates to the product by administrators. Administrators should always promptly deploy Acrobat updates via the enterprise's normal software installation procedure.

Table XVII: Disabling Internet access by the application

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
bUpdater	REG_DWORD	Set to 0 (disable prompting for updates)
bUsageMeasurement	REG_DWORD	Set to 0 (disable sending usage statistics)

3.4. Document Cloud interaction

The "Document Cloud" is a document repository that can be used by Reader to store files and data on Adobe-controlled servers. As with any cloud-based service, it is important to consider the implications of storing data outside of the local network. Federal data should not be stored in a commercial cloud without authorization from the organization and accreditation through the Federal Risk and Authorization Management Program (FedRAMP). Adobe has several products that are FedRAMP Authorized, one being the Adobe Document Cloud [1][2].

Reader includes several features that use cloud storage. Some of which do so without explicit user notification. Reader can be configured to prevent interaction with the Document Cloud. Unless there is a specific need for cloud integration, Reader should be configured to prevent each of these types of interaction as shown in Table XVIII: Disabling Document Cloud services. If one or more cloud services remain enabled, Reader users will have the ability to sign in to the document cloud, allowing the transmission of unspecified data to Adobe.

Table XIX: Disabling Document Cloud services

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices		
bUpdater	REG_DWORD	Set to 0
bToggleAdobeDocumentServices	REG_DWORD	Set to 1
bToggleAdobeSign	REG_DWORD	Set to 1
bTogglePrefSync	REG_DWORD	Set to 1
bToggleWebConnectors	REG_DWORD	Set to 1

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cCloud		
bAdobeSendPluginToggle	REG_DWORD	Set to 1

3.5. Other settings

Reader allows the user to change the default PDF handler, including changing it to a prior version that is still installed on the system that may not have protected mode or protected view enabled. The administrator should disable this feature, as shown in Table XX: Other registry settings, so that the user must use the version with the correct security settings.

Even though Reader stopped supporting Flash® within its product, a user could render the content if a Flash Player is already in place on the system. Since Flash and 3D content have previously been attack vectors, the administrator may want to disable those features as well. Protected mode should mitigate most Flash and 3D content attacks, but if this type of content is not needed, it should be disabled. The administrator should decide based on the needs of the particular environment.

Reader includes several links to subscription-required "upsell" tools by default. Upsell tools extend the functionality of Reader by providing additional functionality like editing PDFs and embedding rich media. NSA has not researched the security of these upsell features but recommends administrators disable them unless there is a need for the features within the organization. In most cases, disabling the features will have no impact on workflow.

Table XXI: Other registry settings

HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown		
bDisablePDFHandlerSwitching	REG_DWORD	Set to 1
bEnableFlash	REG_DWORD	Set to 0
bEnable3D	REG_DWORD	Set to 0
bAcroSuppressUpsell	REG_DWORD	Set to 1

4. Adobe's Customization Wizard and Group Policy

Adobe supplies a Customization Wizard to assist the administrator in deploying Reader across the network. Using the Customization Wizard, the administrator configures the application once, and installs Reader with the same settings on every machine [3].

Many of the registry settings recommended in this configuration guide can be configured with various checkbox settings in the Customization Wizard, but not all. Those that are not directly configured through a specific checkbox in the Customization

Wizard can still be configured with the Customization Wizard tool in the registry settings area. Appendix: Configuring Settings for Adobe's Acrobat Reader DC lists all of the settings from tables 1 through 10 and which section of the Customization Wizard includes those keys. How to use the Customization Wizard to install Reader is beyond the scope of this configuration guide. See the "Adobe Customization Wizard DC for Windows" document for more information, currently at https://www.adobe.com/devnet-docs/acrobatetk/tools/Wizard/.

If the administrator does not want to use the Customization Wizard, a Group Policy can be created to push all desired registry settings across the network. Establishing and deploying a Group Policy is beyond the scope of this configuration guide. However, additional help can be found in the Adobe Application Security Guide. General guidance on deploying Group Policies can be found on Microsoft's support website.

5. Removing previous versions of Adobe Reader

When upgrading Reader, most users will no longer require or use previous versions. In these cases, the best practice is to remove any previous versions before installing Reader. Removing previous versions will prevent users from opening PDF documents with unmaintained software. Adobe's Customization Wizard allows removal of previous versions via a checkbox titled "Remove all versions of Reader" under the "Installation Options".

6. Conclusion

PDFs are commonly exploited by malicious cyber actors. Many security features discussed in this configuration guide can be used to help prevent common attack vectors. Most typical environments can use the Appendix: Configuring Settings for Adobe Acrobat Reader DC as a quick guide to configure Adobe Customization Wizard securely. All administrators should understand the implications of Adobe Reader features and how to lock down the features for secure use of Reader by users of their organization.▪

Works cited

[1] Adobe, Inc., "Acrobat Application Security Guide," 08 June 2021. [Online]. Available: https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html.

[2] Adobe, Inc., "Enterprise Toolkit for Acrobat Products," 2019. [Online]. Available: https://www.adobe.com/devnet-docs/acrobatetk.

[3] Adobe, Inc., "Acrobat DC Customization Wizard DC for Windows," 08 June 2021. [Online]. Available: https://www.adobe.com/devnet-docs/acrobatetk/tools/Wizard/.

Appendix: Configuring Settings for Adobe's Acrobat Reader DC

Registry Key	Data Type	Recommended Value	Customization Wizard	Applies	Default Value	STIG ID
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown						
bEnhancedSecurityStandalone	REG_DWORD	Set to 1	Security	Always	0	64929
bEnhancedSecurityInBrowser	REG_DWORD	Set to 1	Security	Always	0	64955
bProtectedMode	REG_DWORD	Set to 1	Registry	Always	1	64953
iProtectedView	REG_DWORD	Set to 2	Registry	Always	0	64951
bEnableProtectedModeAppContainer	REG_DWORD	Set to 1	Security	Always	0	N/A
bDisableTrustedSites	REG_DWORD	Set to 1	Security	Always (admin may configure trusted sites)	null [0]	65677
iFileAttachmentPerms	REG_DWORD	Set to 1	File Attachments	Always (may relax to 0 if using iUnlistedAttachmentTypePerm)	0	64923
bDisablePDFHandlerSwitching	REG_DWORD	Set to 1	Registry	Always	null [0]	64919
bEnableFlash	REG_DWORD	Set to 0	Registry	Unless required to allow PDFs using Flash	0	64925
bEnable3D	REG_DWORD	Set to 0	Registry	Unless required to allow PDFs using 3D	0	N/A
bUpdater	REG_DWORD	Set to 0	Online Services and Features	Unless end-users manage their own updates	1	N/A
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\<cTrustedFolders>\cAlwaysTrustedForJavaScript						
<tid> (such as t43 or t#)	REG_SZ	Valid path to a file or directory as appropriate	Security	When PDFs from specific directories should be trusted	Null	N/A
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\<cTrustedSites>\cAlwaysTrustedForJavaScript						
<tid> (such as t43 or t#)	REG_SZ	Valid path to host as appropriate	Security	When PDFs from specific hosts should be trusted	Null	N/A
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchAttachmentPerms						

Registry Key	Data Type	Recommended Value	Customization Wizard	Applies	Default Value	STIG ID
iUnlistedAttachmentTypePerm	REG_DWORD	Set to 3	File Attachments	When specific PDFs need to open external apps	1	N/A
tBuiltInPermList	REG_SZ	Default	File Attachments	When specific PDFs need to open external apps	Default	N/A
HKCU\Software\Policies\Adobe\Acrobat Reader\DC\TrustManager\cDefaultLaunchURLPerms						
iURLPerms	REG_DWORD	Set to 1	Registry	Always	1	N/A
tHostPerms	REG_SZ	version:1|<site>:<1-3>| … (1 is always ask; 2 is always allow, 3 is always block)	Registry	When specific PDFs need to be open URLs without a prompt	Null	N/A
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms						
iUnknownURLPerms	REG_DWORD	Set to 3	Registry	Always	1	65667
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cSharePoint						
bDisableSharePointFeatures	REG_DWORD	Set to 1	Registry	Unless SharePoint integration is required	Null [0]	65675
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cWebmailProfiles						
bDisableWebmail	REG_DWORD	Set to 1	WebMail Profiles	Unless end-users send PDFs via Webmail (not Outlook)	Null [0]	64945
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices						
bUpdater	REG_DWORD	Set to 0	Online Services and Features	Unless end-user requires cloud storage	1	65670
bToggleAdobeDocumentServices	REG_DWORD	Set to 1	Online Services and Features	Unless end-user requires cloud storage	null [0]	64927
bToggleAdobeSign	REG_DWORD	Set to 1	Online Services and Features	Unless end-user requires cloud storage	null [0]	64933
bTogglePrefSync	REG_DWORD	Set to 1	Online Services and Features	Unless end-user requires cloud storage	null [0]	64935
bToggleWebConnectors	REG_DWORD	Set to 1	Online Services and Features	Unless end-user requires cloud storage	null [0]	64931

Registry Key	Data Type	Recommended Value	Customization Wizard	Applies	Default Value	STIG ID
HKLM\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cCloud						
bAdobeSendPluginToggle	REG_DWORD	Set to 1	Online Services and Features	Unless end-user requires cloud storage	1	64921
HKCU\Software\Adobe\Acrobat Reader\DC\TrustManager						
bEnableAlwaysOutlookAttachmentProtectedView	REG_DWORD	Set to 0	Registry	Always	0	N/A