National Security Agency/Central Security Service

Information Assurance Directorate

Recommendations for Configuring Adobe Acrobat Reader XI in a Windows Environment

July 12, 2013
Revision 1

A product of the Network Components and Applications Division

TSA-13-1021-SG

Contents

1 Introduction 1

2 The Sandbox and Enhanced Security 1

3 Privileged Locations 3

4 Attachments 4

5 Internet Access from a Document via Hyperlink 5

6 JavaScript 6

7 Internet Access from the ARXI Application 7

8 Other Settings 8

9 Adobe's Customization Wizard and Group Policy 9

10 References 10

11 Appendix A – Customization Wizard 11

12 Appendix B – PowerShell 15

List of Tables

Table 1: Configure and lock Enhanced Security, Protected Mode, and Protected View 3

Table 2: Lock privileged locations 4

Table 3: Disable attachments 4

Table 4: Whitelisting attachment types 5

Table 5: Restrict hyperlinks 5

Table 6: Disable JavaScript and enable trusted locations 6

Table 7: Disable online service access 8

Table 8: Disable Internet access by the application 8

Table 9: Other registry settings 9

Disclaimer

This Guide is provided "as is." Any express or implied warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the United States Government be liable for any direct, indirect, incidental, special, exemplary or consequential damages (including, but not limited to, procurement of substitute goods or services, loss of use, data or profits, or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this Guide, even if advised of the possibility of such damage.

The User of this Guide agrees to hold harmless and indemnify the United States Government, its agents and employees from every claim or liability (whether in tort or in contract), including attorneys' fees, court costs, and expenses, arising in direct consequence of Recipient's use of the item, including, but not limited to, claims or liabilities made for injury to or death of personnel of User or third parties, damage to or destruction of property of User or third parties, and infringement or other violations of intellectual property or technical data rights.

Nothing in this Guide is intended to constitute an endorsement, explicit or implied, by the U.S. Government of any particular manufacturer's product or service.

Trademark Information

This publication has not been authorized, sponsored, or otherwise approved by Adobe Systems Incorporated.

Microsoft®, Windows®, PowerShell®, Office® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat®, Reader®, and Adobe PDF® are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

1 Introduction

The greatest threat to users of Adobe Acrobat Reader is opening a PDF file that contains malicious executable content. The risk of a user receiving such a document through email or web surfing is high. Phishing attacks frequently include malicious PDF attachments. Adobe Acrobat Reader X and XI run in a sandboxed process to protect the user from malicious documents. This paper contains recommended configuration settings for United States Government and Department of Defense administrators for Adobe Acrobat Reader XI (ARXI) to minimize executable content and other attacks in a Microsoft Windows environment.

ARXI settings fall into two broad types – those that should be used in all environments, and those for environments with unique security requirements. Sections 2 through 5 describe the settings applicable to all environments. These should have minimal impact to workflow and productivity yet provide some protections against malicious executable content. Sections 6 through 8 describe settings that should be tailored to the specific security needs of the environment since these settings will impact workflow and productivity.

Acrobat's digital signature capabilities and related settings are beyond the scope of this paper. Administrators that need to configure these specialized settings should consult Adobe's website for their latest digital signature guidance. This document includes information for using Adobe's Customization Wizard (CW) or Microsoft's PowerShell to configure the necessary settings for uniform distribution of the software throughout an enterprise or on a standalone system. Appendix A lists all of the ARXI security-related settings with recommendations for the environments that should configure those settings.

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-relevant patches and updates.

2 The Sandbox and Enhanced Security

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. ARXI includes two sandboxing options: protected mode and protected view. Another critical mechanism is enhanced security.

> **Protected Mode** – When protected mode is enabled, Acrobat opens the PDF document in the sandbox with the executable content (e.g. JavaScript) enabled, but the content is restricted in what it can do and access. 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 according to certain limits.

Prior to the inclusion of the protected mode sandbox, the typical security practice was to disable all JavaScript to prevent execution of malicious scripts. Protected mode differs greatly from just disabling JavaScript because the document is opened in a sandboxed state. The constrained execution environment limits all actions, not just those within scripts, and can block much malicious activity.

Protected View – Protected view, new to Reader in version XI, is a more restrictive sandbox than protected mode. When protected view is enabled, Acrobat opens the PDF document with executable content and scripts disabled. The user can still view the document and will see a Yellow Message Bar (YMB) across the top with a warning that some features of the document have been disabled, as shown here:

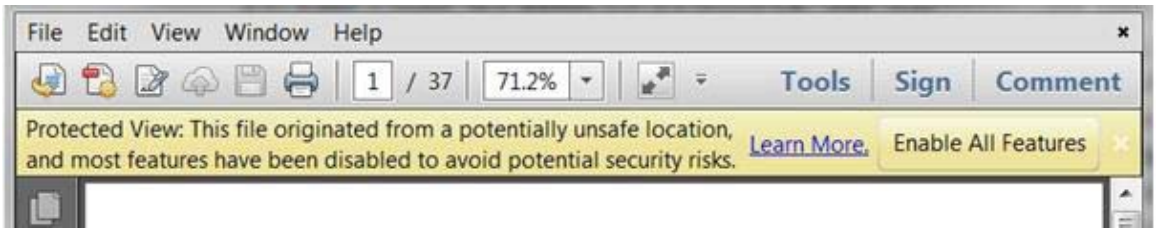

Figure 1: The Protected View Yellow Message Bar

The user has the option to enable those features after deciding whether to trust the document and whether those features are necessary.

Protected view is essential to prevent users from inadvertently opening and executing malicious active content. Requiring the user to view the document prior to enabling active content can prevent many phishing and other attacks. Once the user views the document and enables the content, ARXI adds the document as a privileged location (see next section) for that user and bypasses protected view on subsequent opens of that document. The document will still be subject to the protected mode sandbox if protected mode is enabled.

Enhanced Security – Enhanced security enforces some essential security elements which help to protect users. According to Adobe's documentation, Enhanced Security:

- Prevents cross domain access: requested content must adhere to a "same-origin" policy. Without a server-based cross domain policy file, that content is blocked.

- Blocks stream access to Xobjects, silent printing, execution of high privilege JavaScript, and script/data injection for PDF not requested by the PDF.

ARXI includes a registry key under the HKLM hive, *FeatureLockDown*, for administrators to configure certain security settings. Values under *FeatureLockDown* do not necessarily disable functionality. The purpose of *FeatureLockDown* is to prevent the user from changing settings through the ARXI GUI. Some of the same settings are also under HKCU, but configuring those under HCKU alone is not recommended because HKCU is writeable by the user.

Enhanced security and protected mode are turned on by default in ARXI, but they are not locked, meaning a user can disable them through the GUI. Protected view is not turned on by default. All three should be enabled and locked as shown in Table 1 for all environments. This should have minimal impact to productivity and workflow, and if necessary, the administrator can use privileged locations for exceptions (See section 3).

HKLM\Software\Policies\Adobe\<product>\<version>\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
HKCU\Software\Adobe\<product>\<version>\TrustManager		
bEnableAlwaysOutlookAttachmentProtectedView	REG_DWORD	Set to 0
bDisableTemporaryFileProtectedView	REG_DWORD	Set to 0

Table 1: Configure and lock Enhanced Security, Protected Mode, and Protected View

The setting *bEnableAlwaysOutlookAttachmentProtectedView* from the Table 1 only applies to attachments received from Microsoft Outlook in Office 2010 and later. Previous versions of Outlook do not append origin information to attachments.

3 Privileged Locations

Privileged Locations allow the user to selectively trust files, folders, and hosts 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)*). The administrator can disable the user's ability to create privileged locations through the Preferences dialog by using the settings in Table 2. By disabling the GUI options to create privileged locations and enabling protected mode/protected view/enhanced security as described in Table 1 above, the user will be required to first view all documents with active content disabled and to take explicit action to enable active content. The user will not be able to preemptively exempt specific documents or locations through the GUI.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown		
bDisableOSTrustedSites	REG_DWORD	Set to 1
bDisableTrustedFolders	REG_DWORD	Set to 1
bDisableTrustedSites	REG_DWORD	Set to 1
bEnableCertificateBasedTrust	REG_DWORD	Set to 0

Table 2: Lock privileged locations

The settings in Table 2 prevent the user from directly adding sites and folders 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 ARXI will create a privileged location for just that file for that user for later use. If workflow is impacted, the administrator can create privileged locations as needed for the user (see the Acrobat Application Security Guide). The administrator can also leverage Internet Explorer (IE) trusted sites as privileged locations, or can allow the user to preemptively trust documents with valid certification. Table 2 shows the most restrictive settings, but with careful planning for certificate trust chain and the IE Zones, the administrator can relax the settings for *bDisabledOSTrustedSites* and *bEnableCertificateBasedtrust*.

4 Attachments

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 3.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown		
iFileAttachmentPerms	REG_DWORD	Set to 1

Table 3: Disable attachments

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 blacklist or whitelist. In most environments, there is little use for attachments to PDF documents and this setting will not affect workflow. In environments where users need collaborative document sharing capabilities, this setting could affect productivity.

A less restrictive but manageable approach is to set *iFileAttachmentPerms* to 0 and to allow only certain types of attachments. ARXI allows the administrator to blacklist/whitelist specific attachment types and to automatically blacklist unlisted types.

When using a blacklist/whitelist mechanism, the recommended approach is block everything and allow approved exceptions. To do this in ARXI, disable unlisted attachment types with

iUnlistedAttachmentTypePerm and then enable only those that are safe or needed with *tBuiltInPermList*. Table 4 shows the necessary settings.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown		
iFileAttachmentPerms	REG_DWORD	Set to 0 or not defined
HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cDefaultLaunchAttachmentPerms		
iUnlistedAttachmentTypePerm	REG_DWORD	Set to 3
tBuiltInPermList	REG_SZ	version:1|<extension>:<0-3>| …

Table 4: Whitelisting attachment types

To allow a *.docx* file 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. ARXI is installed with a default list of extensions that an administrator can customize in the registry or the Customization Wizard.

5 Internet Access from a Document via Hyperlink

PDF documents can contain hyperlinks to files or web sites which could lead a user to malicious content. By default, a PDF file cannot send information to the Internet when a user tries to follow a hyperlink within a document, but the user can change these settings through the GUI (*Edit → Preferences → Trust Manager*, button labeled "Change Settings" in the Internet Access section). The administrator can prevent the user from changing the default setting by using the *FeatureLockDown* key as in Table 5 and if desired can block all access to hyperlinks from within a document.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cDefaultLaunchURLPerms		
iURLPerms	REG_DWORD	Set to 1
HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cDefaultLaunchURLPerms		
iUnknownURLPerms	REG_DWORD	Set to 2 (prompt user for unlisted sites) or Set to 3 (block all unlisted sites)
tHostPerms	REG_SZ	version:1|<site>:<1 -3>| … (1 is always ask; 2 is always allow, 3 is always block)

Table 5: Restrict hyperlinks

The recommended approach is to set *iUnknownURLPerms* to 2 which warns the user before following a hyperlink. The user will know that a hyperlink was activated and that the PDF is trying to access the Internet. If needed, the administrator could set *iUnknownURLPerms* to 3 blocking hyperlinks to all sites not explicitly whitelisted and use tHostPerms to whitelist approved site hyperlinks but this approach requires more administration.

6 JavaScript

For those environments where JavaScript must be disabled, the most restrictive configuration is to:

- set protected mode, protected view and enhanced security as suggested in Table 1 (Section 2),
- lock the privileged location settings as suggested in Table 2 (Section 3),
- disable JavaScript and establish trusted locations for particular documents that the user needs as in Table 6 below.

With this configuration, the user will not be able to execute any JavaScript in any PDF file outside of those locations and will not be able to change the setting through the ARXI GUI. The administrator can add particular files, directories, drives, or hosts as trusted locations which 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.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown		
bDisableJavaScript	REG_DWORD	Set to 1
HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\<cTrustedFolders or cTrustedSites>\cAlwaysTrustedForJavaScript		
<tid> (such as t43 or t#)	REG_SZ	Valid path to a file, directory or host as appropriate

Table 6: Disable JavaScript and enable trusted locations

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. For environments where workflow is severely impacted by the most restrictive JavaScript settings, ARXI includes a less restrictive configuration: enable JavaScript, enable and lock protected view, protected mode, and enhanced security as described in Section 2, and allow the user to trust a document after first viewing it within protected view where JavaScript is disabled. The presumption with this approach is that the user will be able to determine the authenticity of the document after viewing the contents and will know whether

it is safe to trust the active content. This configuration strikes a reasonable balance between risk and functionality.

An administrator has further granularity with the ability to create white and black lists for particular JavaScript APIs. Generally, this requires serious administrative investment and is not a scalable/manageable solution. It is practical only for installations where there is a specific need for this level of granularity beyond the basic recommendations (See the Acrobat Application Security Guide to use this feature).

7 Internet Access from the ARXI Application

ARXI includes features to enable access to online services such as Adobe.Com, Adobe EchoSign, Office 365, SendNow, 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 (e.g. gmail, yahoo). Most of this capability can be blocked by using the settings in Table 7. These settings should be tailored for individual environments since they will block many useful features of ARXI.

ARXI allows the user to configure a webmail account to send an open PDF document as an attachment. Users already had the ability to send documents as Microsoft Outlook attachments. The difference is that Outlook must be configured by the administrator on the local machine. If Outlook is not configured, the user cannot use it from within Acrobat. Webmail access would allow the user to bypass the need for Outlook and go right to a webmail solution, which may or may not be something the administrator wants to allow. Some installations will need to block access to webmail.

Removing the Sign pane prevents the user from using Adobe's EchoSign service from within ARXI. Users will still have the ability to sign a document with a local digital signature solution, or to sign documents that already have signature blocks in them.

HKCU\Software\Adobe\<product>\<version>\Workflows		
bEnableAcrobatHS	REG_DWORD	Set to 0
bEnableRTCPart	REG_DWORD	Set to 0
bEnableRTCAuth	REG_DWORD	Set to 0
bEnableShareFile	REG_DWORD	Set to 0
bEnableDocCtrInit	REG_DWORD	Set to 0
HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\cSharePoint		
bDisableSharePointFeatures	REG_DWORD	Set to 1 (also disables Office 365)

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\cCloud		
bDisableADCFileStore	REG_DWORD	Set to 1
HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\cServices		
bEnableSignPane	REG_DWORD	Set to 0
HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\cWebmailProfiles		
bDisableWebmail	REG_DWORD	Set to 1

Table 7: Disable online service access

The ARXI application also accesses the Internet for a few other tasks, such as the displaying commercial ads and product registration. These settings should be disabled in environments where the administrator needs to restrict all unnecessary Internet access by an application, as shown in Table 8.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown		
bCommercialPDF	REG_DWORD	Set to 1
bRegisterProduct	REG_DWORD	Set to 1
bShowAdsAllow	REG_DWORD	Set to 1
bPurchaseAcro	REG_DWORD	Set to 0
bShowEbookMenu	REG_DWORD	Set to 0
bUpdater	REG_DWORD	Set to 0 (disable prompting for updates)
bUsageMeasurement	REG_DWORD	Set to 0 (disable sending usage statistics)

Table 8: Disable Internet access by the application

Currently, ARXI requires the system administrator to update the product, users cannot update and do not need to see the update notifications. Disabling the automatic update feature for users will prevent ARXI 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.

8 Other Settings

ARXI 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 9, so that the user must use the version with the correct security settings.

Since Flash and 3D content have been attack paths in the past, the administrator may want to disable those features as well. Protected mode should mitigate 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.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown		
bDisablePDFHandlerSwitching	REG_DWORD	Set to 1
bEnableFlash	REG_DWORD	Set to 0
bEnable3D	REG_DWORD	Set to 0

Table 9: Other registry settings

9 Adobe's Customization Wizard and Group Policy

Adobe supplies a Customization Wizard (CW) to assist the administrator in deploying Adobe Reader across the network. Using the CW, the administrator configures the application once, and installs ARXI with the same settings on every machine. Many of the registry settings recommended in this paper can be configured with various checkbox settings in the CW, but not all. Those that are not directly configured through a specific checkbox in the CW can still be configured with the CW tool in the registry settings. Appendix A lists all of the settings from Tables 1 through 9 and which section of the CW includes those keys. How to use the CW to install ARXI is beyond the scope of this paper. See the Adobe Customization Wizard XI for Windows document for more information, currently hosted at http://www.adobe.com/devnet-docs/acrobatetk.

If the administrator does not want to use the CW, Adobe released a Group Policy template for ARXI. This template includes very few of the recommended settings from this paper, but the administrator can add settings and use Group Policy to push all the desired registry settings across the network. The Enterprise Toolkit on the Adobe website hosts FTP directories for all Adobe Reader installers. The direct link to the FTP site is currently ftp://ftp.adobe.com/pub/adobe. Additionally, Appendix B contains a PowerShell script to configure the recommended settings in this guide. The administrator needs to tailor a few settings before running the script.

10 References

Adobe hosts the following references in the Enterprise Toolkit for Acrobat Products, http://www.adobe.com/devnet-docs/acrobatetk

- Adobe Acrobat Application Security Guide (also available as a standalone PDF from http://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/Acrobat Application Security Guide.pdf)
- Adobe Customization Wizard XI for Windows
- Preference Reference (direct link http://www.adobe.com/devnet-docs/acrobatetk/tools/PrefRef/Windows/index.html)

11 Appendix A – Customization Wizard

This section includes the settings listed in Tables 1 through 9 with additional columns indicating where to find the setting in Adobe's Customization Wizard and the recommendation for use of the setting in different environments. Administrators in all environments should review the Optional settings and use those that apply to their enterprise.

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown				**Recommended Environment**
bEnhancedSecurityStandalone	REG_DWORD	Set to 1	Security Tab	All environments
bEnhancedSecurityInBrowser	REG_DWORD	Set to 1	Security Tab	All environments
bProtectedMode	REG_DWORD	Set to 1	Registry Tab	All environments
iProtectedView	REG_DWORD	Set to 2	Registry Tab	All environments
bDisableOSTrustedSites	REG_DWORD	Set to 1	Registry Tab	All environments (may relax to 0 with use of IE Zones)
bDisableTrustedFolders	REG_DWORD	Set to 1	Security Tab *	All environments (admin may configure trusted folders)
bDisableTrustedSites	REG_DWORD	Set to 1	Security Tab *	All environments (admin may configure trusted sites)
bEnableCertificateBasedTrust	REG_DWORD	Set to 0	Registry Tab	Environments with Certificate Trust Chain
bDisableJavaScript	REG_DWORD	Set to 1	Registry Tab	Optional
iFileAttachmentPerms	REG_DWORD	Set to 1	File Attachments Tab	All environments (may relax to 0 if using iUnlistedAttachmentTypePerm)
bCommercialPDF	REG_DWORD	Set to 1	Online and Adobe online services Features Tab	Optional
bRegisterProduct	REG_DWORD	Set to 1	Registry Tab	Optional

bShowAdsAllow	REG_DWORD	Set to 1	Registry Tab	Optional
bPurchaseAcro	REG_DWORD	Set to 0	Online and Adobe online services Features Tab	Optional
bShowEbookMenu	REG_DWORD	Set to 0	Online and Adobe online services Features Tab	Optional
bUpdater	REG_DWORD	Set to 0	Online and Adobe online services Features Tab	Optional
bUsageMeasurement	REG_DWORD	Set to 0	Online and Adobe online services Features Tab	Optional
bDisablePDFHandlerSwitching	REG_DWORD	Set to 1	Registry Tab	All environments
bEnableFlash	REG_DWORD	Set to 0	Registry Tab	Optional
bEnable3D	REG_DWORD	Set to 0	Registry Tab	Optional

*Specific folders or hosts to trust can be configured through the Security Tab

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ <cTrustedFolders>\cAlwaysTrustedForJavaScript				**Recommended Environment**
<tid> (such as t43 or t#)	REG_SZ	Valid path to a file, directory or host as appropriate	Registry Tab	where JavaScript is disabled (admin may configure trusted sites and folders)

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ <cTrustedSites>\cAlwaysTrustedForJavaScript				**Recommended Environment**
<tid> (such as t43 or t#)	REG_SZ	Valid path to a file, directory or host as appropriate	Registry Tab	where JavaScript is disabled (admin may configure trusted sites and folders)

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cDefaultLaunchAttachmentPerms (use if iFileAttachmentPerms is set to 0 or not configured)				**Recommended Environment**
iUnlistedAttachmentTypePerm	REG_DWORD	Set to 3	File Attachments Tab	where iFileAttachmentPerms is set to 0
tBuiltInPermList	REG_SZ	version:1|<extension>:<0-3>| …	File Attachments Tab	where iFileAttachmentPerms is set to 0

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cDefaultLaunchURLPerms				**Recommended Environment**
iURLPerms	REG_DWORD	Set to 1	Registry Tab	All environments
iUnknownURLPerms	REG_DWORD	Set to 3 (block all unlisted sites) or 2 (prompt user for unlisted sites)	Registry Tab	All environments, set to 2 at least
tHostPerms	REG_SZ	version:1|<site>:<1-3>| … (1 is always ask; 2 is always allow, 3 is always block)	Registry Tab	All environments

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cSharePoint				**Recommended Environment**
bDisableSharePointFeatures	REG_DWORD	Set to 1	Registry Tab	Optional

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\cCloud				**Recommended Environment**
bDisableADCFileShare	REG_DWORD	Set to 1	Registry Tab	Optional

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\ cWebmailProfiles				**Recommended Environment**
bDisableWebmail	REG_DWORD	Set to 1	Webmail Profiles Tab	Optional

HKLM\Software\Policies\Adobe\<product>\<version>\FeatureLockDown\cServices				Recommended Environment
bEnableSignPane	REG_DWORD	Set to 0	Registry Tab	Optional

HKCU\Software\Adobe\<product>\<version>\TrustManager				Recommended Environment
bEnableAlwaysOutlookAttachmentProtectedView	REG_DWORD	Set to 0	Registry Tab	All environments
bDisableTemporaryFileProtectedView	REG_DWORD	Set to 0	Registry Tab	All environments

HKCU\Software\Adobe\<product>\<version>\Workflows				Recommended Environment
bEnableAcrobatHS	REG_DWORD	Set to 0	Online and Adobe online services Features Tab	Optional
bEnableRTCPart	REG_DWORD	Set to 0	Online and Adobe online services Features Tab	Optional
bEnableRTCAuth	REG_DWORD	Set to 0	Registry Tab	Optional
bEnableShareFile	REG_DWORD	Set to 0	Registry Tab	Optional
bEnableDocCtrInit	REG_DWORD	Set to 0	Registry Tab	Optional

12 Appendix B – PowerShell

The following PowerShell script will configure all the settings as recommended in Appendix A, including those that are optional. The script should be adjusted based on environmental needs. This script is designed to run locally on a single machine and requires administrative rights.

To use this script, the administrator will need to configure several strings. The administrator should search for these in the script and replace “” with an appropriate value, also replacing *someTID* with an appropriate value. The affected settings are *cAlwaysTrustedForJavaScript, tBuiltinPermList, tHostPerms.*

```
function Create-RegProperty($key, $name, $type, $value){
    if((Test-Path $key) -eq $FALSE){
        $parent = Split-Path -parent $key
        $child = Split-Path -leaf $key
        Create-RegKey $parent $child
    }
    New-ItemProperty -Path $key -Name $name -PropertyType $type -Value $value -
ErrorAction silentlycontinue -force

}

function Create-RegKey($parent, $child){
    #assumes root path (HKCU, HKLM, ...) of $parent exists
    if((Test-Path $parent) -eq $FALSE){
        $grandParent = Split-Path -parent $parent
        $parentLeaf = Split-Path -leaf $parent
        Create-RegKey $grandParent $parentLeaf | Out-Null
    }

    $newKey = Join-Path $parent $child

    if((Test-Path $newKey) -eq $FALSE){
        New-Item -path $newKey | Out-Null
    }

}

function Create-FeatureLockDownKeys(){
    $FeatureLockDown_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown"

    Create-RegProperty $FeatureLockDown_key "bEnhancedSecurityStandalone" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bEnhancedSecurityInBrowser" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bProtectedMode" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "iProtectedView" "DWORD" 2
    Create-RegProperty $FeatureLockDown_key "bDisableOSTrustedSites" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bDisableTrustedFolders" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bDisabledTrustedSites" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bEnableCertificateBasedTrust" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bDisableJavaScript" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "iFileAttachmentPerms" "DWORD" 1
```

```
    Create-RegProperty $FeatureLockDown_key "bCommercialPDF" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bRegisterProduct" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bShowAdsAllow" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bPurchaseAcro" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bShowEbookMenu" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bUpdater" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bUsageMeasurement" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bDisablePDFHandlerSwitching" "DWORD" 1
    Create-RegProperty $FeatureLockDown_key "bEnableFlash" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bEnable3d" "DWORD" 0
    Create-RegProperty $FeatureLockDown_key "bBrowserIntegration" "DWORD" 0
}

function Create-cAlwaysTrustedForJavaScript(){
       #THESE KEYS ARE JUST PLACEHOLDS AND NEED TO BE MANUALLY SET.
       #"someTID" --> t<somenumber)
       #"somePath" --> path\to\valid\file\or\directory
    $cAlwaysTrustedForJavaScript_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cTrustedSites\cAlwaysTrustedForJavaScript"
    Create-RegProperty $cAlwaysTrustedForJavaScript_key "someTID" "STRING"
"somePath"

    $cAlwaysTrustedForJavaScript_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cTrustedFolders\cAlwaysTrustedForJavaScript"
    Create-RegProperty $cAlwaysTrustedForJavaScript_key "someTID" "STRING"
"somePath"
}

function Create-cDefaultLaunchAttachmentPerms(){
    $cDefaultLaunchAttachmentPerms_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cDefaultLaunchAttachmentPerms"
    Create-RegProperty $cDefaultLaunchAttachmentPerms_key
"iUnlistedAttachmentTypePerm" "DWORD" 3
    Create-RegProperty $cDefaultLaunchAttachmentPerms_key "tBuiltinPermList"
"STRING" ""
}

function Create-cDefaultLaunchURLPerms(){
    $cDefaultLaunchURLPerms_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cDefaultLaunchURLPerms"
    Create-RegProperty $cDefaultLaunchURLPerms_key "iURLPerms" "DWORD" 1
    Create-RegProperty $cDefaultLaunchURLPerms_key "iUnknownURLPerms" "DWORD" 3
    Create-RegProperty $cDefaultLaunchURLPerms_key "tHostPerms" "STRING" ""
}

function Create-cSharePoint(){
    $cSharePoint_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cSharePoint"
    Create-RegProperty $cSharePoint_key "bDisableSharePointFeatures" "DWORD" 1
}

function Create-cCloud(){
    $cCloud_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cCloud"
    Create-RegProperty $cCloud_key "bDisableADCFileShare" "DWORD" 1
```

```
}

function Create-cWebMailProfiles(){
    $cWebMailProfiles_key = "HKLM:\Software\Policies\Adobe\Acrobat
Reader\11.0\FeatureLockDown\cWebmailProfiles"
    Create-RegProperty $cWebMailProfiles_key "bDisableWebmail" "DWORD" 1
}

function Create-TrustManager(){
    $trustManager_key = "HKCU:\Software\Adobe\Acrobat Reader\11.0\TrustManager"
    Create-RegProperty $trustManager_key
"bEnableAlwaysOutlookAttachmentProtectedView" "DWORD" 0
    Create-RegProperty $trustManager_key "bDisableTemporaryFileProtectedView"
"DWORD" 0
}

function Create-WorkFlows(){
    $workFlows_key = "HKCU:\Software\Adobe\Acrobat Reader\11.0\WorkFlows"
    Create-RegProperty $workFlows_key "bEnableAcrobatHS" "DWORD" 0
    Create-RegProperty $workFlows_key "bEnableRTCPart" "DWORD" 0
    Create-RegProperty $workFlows_key "bEnableRTCAuth" "DWORD" 0
    Create-RegProperty $workFlows_key "bEnableShareFile" "DWORD" 0
    Create-RegProperty $workFlows_key "bEnableDocCtrInit" "DWORD" 0
}

function Main(){
    Create-FeatureLockDownKeys
    Create-cAlwaysTrustedForJavaScript
    Create-cDefaultLaunchAttachmentPerms
    Create-cDefaultLaunchURLPerms
    Create-cSharePoint
    Create-cCloud
    Create-cWebMailProfiles
    Create-TrustManager
    Create-WorkFlows
}

Main
```