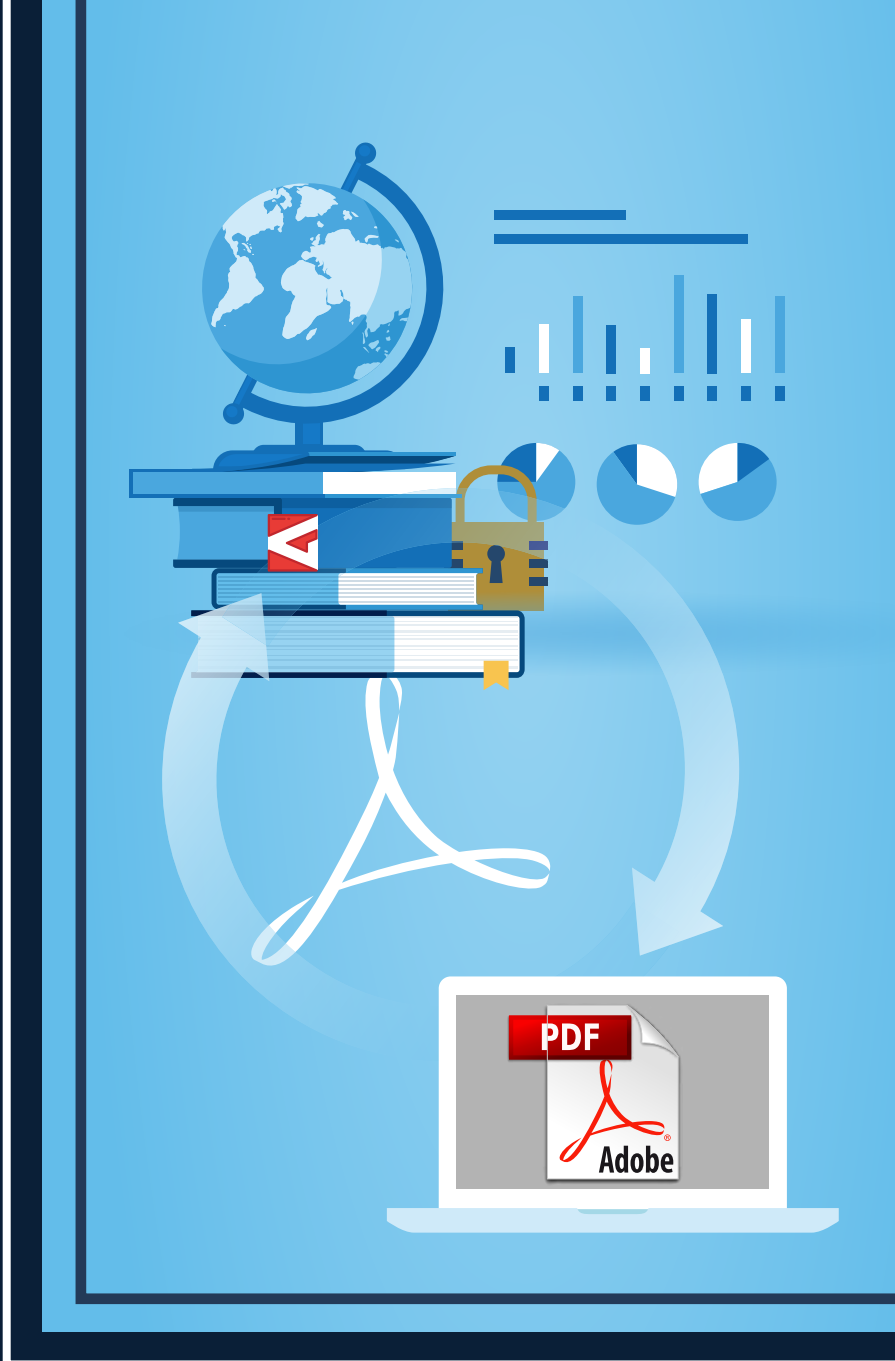


CCN-CERT BP/16



Security recommendations of Adobe Acrobat Reader DC

GOOD PRACTICE REPORT

MARCH 2022

ccn-cert
centro criptológico nacional

CCN
centro criptológico nacional

Edited by:



Paseo de la Castellana 109, 28046 Madrid

© National Cryptology Centre, 2022

Issue Date: March, 2022

LIMITATION OF LIABILITY

This document is provided in accordance with the terms contained herein, expressly rejecting any type of implicit guarantee that may be related to it. Under no circumstances can the National Cryptologic Centre be held responsible for direct, indirect, fortuitous or extraordinary damage derived from the use of the information and software indicated, even when warned of such a possibility.

LEGAL NOTICE

The reproduction of all or part of this document by any means or process, including reprography and computer processing, and the distribution of copies by public rental or loan, is strictly prohibited without the written authorisation of the National Cryptologic Centre, subject to the penalties established by law.

Index

| | |
|--|----|
| 1. About CCN-CERT, National Governmental Cert | 4 |
| 2. Introduction | 5 |
| 3. Installing and bashing Adobe Reader DC continuous track on Windows | 6 |
| 3.1. Download and install Adobe Reader dc continuous track | 7 |
| 3.2. Versions | 8 |
| 3.3. Requirements | 9 |
| 3.4. Location of the installation | 10 |
| 3.5. Downloading and installing Reader | 11 |
| 3.5.1. Acrobat Reader DC (Enterprise) | 11 |
| 3.5.2. Acrobat Reader DC (individuals) | 12 |
| 3.6. Apply security values | 13 |
| 3.6.1. Windows client | 13 |
| 3.6.2. Windows server, how to create and manage the central repository for group policy administrative templates | 14 |
| 3.7. Register values | 15 |
| 3.8. Disable the adobe acrobat update task | 29 |
| 3.9. Disable "Adobearmservice" service | 30 |
| 4. Checklist (assessment) | 31 |
| 5. Decalogue of recommendations | 33 |
| ANNEX. Secure configuration scripts | 34 |

1. About CCN-CERT, National Governmental Cert

The CCN-CERT is the Information Security Incident Response Capacity of the National Cryptologic Centre, CCN, attached to the National Intelligence Centre, CNI. This service was created in 2006 as the **Spanish National Governmental CERT** and its functions are set out in Law 11/2002 regulating the CNI, RD 421/2004 regulating the CCN and in RD 3/2010, of 8 January, regulating the National Security Framework (ENS), modified by the RD 311/2022 of 3 May.

Its mission, therefore, is to contribute to the improvement of Spanish cybersecurity, being the national alert and response centre that cooperates and helps to respond quickly and efficiently to cyber-attacks and to actively face cyber-threats, including the coordination at state public level of the different existing Incident Response Capabilities or Cybersecurity Operations Centres.

All of this, with the ultimate aim of achieving a safer and more reliable cyberspace, preserving classified information (as stated in art. 4. F of Law 11/2002) and sensitive information, defending Spain's Technological Heritage, training expert personnel, applying security policies and procedures and using and developing the most appropriate technologies for this purpose.

In accordance with these regulations and Law 40/2015 on the Public Sector Legal Set of rules, the CCN-CERT is responsible for the management of cyber-incidents affecting any public body or company. In the case of critical public sector operators, cyber-incident management will be carried out by the CCN-CERT in coordination with the CNPIC.

**The CCN-CERT is the
Information Security
Incident Response
Capacity of the National
Cryptologic Centre**

2. Introduction

This document is part of the documentation issued by the National Cryptologic Centre whose objective is to preserve the security of the ICT systems of the Public Administrations.

To this end, a mechanism is provided to apply security measures in an automated and unattended way on a PDF file viewing software, to facilitate the possibility of implementing security in ICT systems in a simple and agile way.

Object

The purpose of this document is to set out the procedures and utilities necessary to implement and ensure security in Adobe Reader DC continuing release.

Scope

This document sets out a procedure to enhance security and protect Adobe Acrobat Reader DC to mitigate potential vulnerabilities and risks to which it may be exposed.

Users of this guide can enhance the security of this application through the user interface and Registry settings, as well as configure features of this product to protect the integrity of PDF content.

This document is part of the documentation issued by the National Cryptologic Centre whose objective is to preserve the security of the ICT systems of the Public Administrations



Adobe Acrobat DC

3. Installing and bashing Adobe Reader DC continuous track on Windows

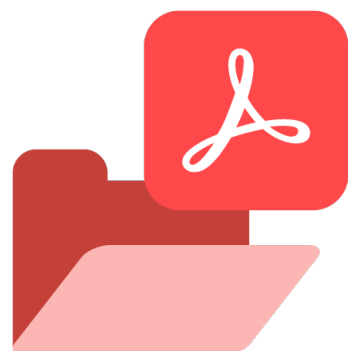
Adobe Reader is available for free download from Adobe's website and allows viewing and printing of PDF documents.

This manual is designed for Adobe Acrobat Reader DC Continuous Track, but can also be used for later versions.

Adobe Reader DC must have the latest security-related software updates installed. To do so, determine the update method (e.g. connection to a WSUS server, local procedure, automatic update, etc.).

To determine which version you have installed, click Help >> About Adobe Acrobat Reader DC. Verify that you have the latest software update applied. If the latest Adobe security-related software updates are not applied, this would be a critical security flaw.

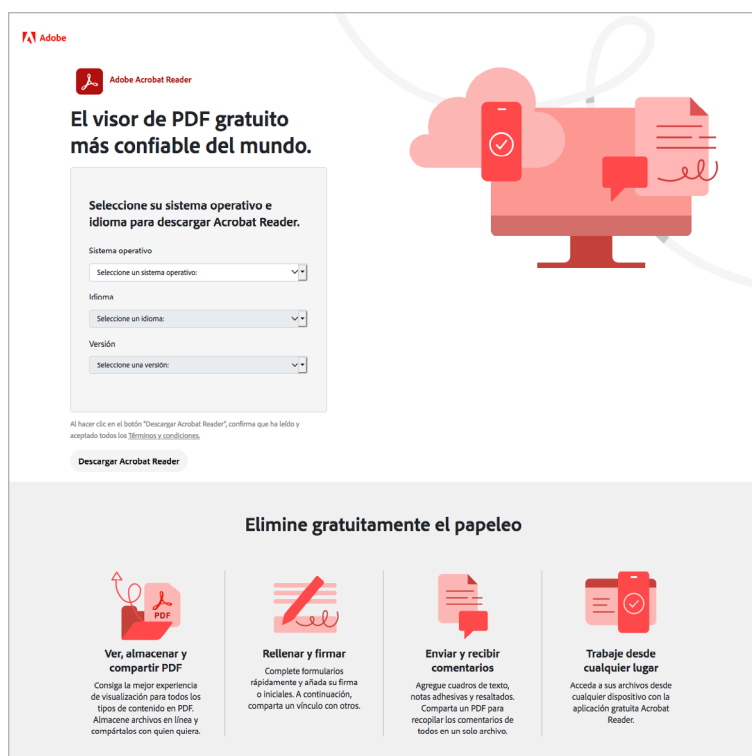
Adobe Reader is available for free download from Adobe's website



3.1. Download and install Adobe Reader dc continuous track

The programme must be downloaded from a computer connected to the internet.

Before downloading the programme, please note the following information.



3.2. Versions

The Acrobat Reader DC desktop software is available for deployment with both the "classic" and "continuous" versions.

The "continuous" version provides service-based tools, as well as new features, security and platform enhancements, and bug fixes more frequently. The update cadence of the continuous track is more frequent than the classic track.

The "classic" version is similar to the 10.X - 11.X model and does not provide new features in upgrades. Free services are available, but optional. The update cadence is quarterly and provides security and platform improvements as well as bug fixes.

Below, we can see the generic format for displaying the final version of Adobe Reader DC (major.minor.minor_minor).

The Acrobat Reader DC desktop software is available for deployment with both the "classic" and "continuous" versions

| DESCRIPTION | | |
|--|-------------------|---|
| <div><div>Release Year</div><div>Track ID</div><div>Hidden change list field</div><div>15.006.20456.110321</div><div>Internal build #</div><div>Internal build #</div></div> | | |
| VERSION | RANGE | NOTES |
| Larger | 1-255 | The last two digits of the release year |
| Less | 1-255 | An internal number indicating when the code is moved from Trunk to Beta |
| Less_less | 1-65535 | The first two digits indicate the version: 20=Continuous; 30=Classic |
| 4th hidden field | Changelist number | Only visible if user clicks on the version number in the "About" box |

3.3. Requirements

The following are the minimum system requirements necessary to implement Adobe Acrobat Reader DC.

| | |
|------------------------------------|---|
| Acrobat Reader DC (32 bits) | <ul style="list-style-type: none">▶ 1.5 GHz Intel® or AMD processor or faster▶ Windows 11 (64-bit), Windows 10 (32-bit and 64-bit) version 1809 or later, Windows 8, 8.1 (32-bit and 64-bit) *, Windows 7 SP1 (32-bit and 64-bit) or Windows Server - 2008 R2 (64-bit), 2012 (64-bit), 2012 R2 (64-bit) *, 2016 (64-bit) or 2019 (64-bit)▶ 2 GB RAM▶ 450 MB of available hard disk space▶ Display resolution of 1024 × 768▶ Internet Explorer 11 |
|------------------------------------|---|

[*] With Windows 2919355 installed.

| | |
|------------------------------------|--|
| Acrobat Reader DC (64 bits) | <ul style="list-style-type: none">▶ 1.5 GHz Intel® or AMD processor or faster▶ Windows 11 (64-bit), Windows 10 (64-bit) version 1809 or later, Windows Server 2016 (64-bit), or Windows Server 2019 (64-bit)▶ 2 GB RAM▶ 900 MB of available hard disk space for English▶ 1 GB of available hard disk space for other languages▶ Display resolution of 1024 × 768▶ Internet Explorer 11 |
|------------------------------------|--|

3.4. Location of the installation

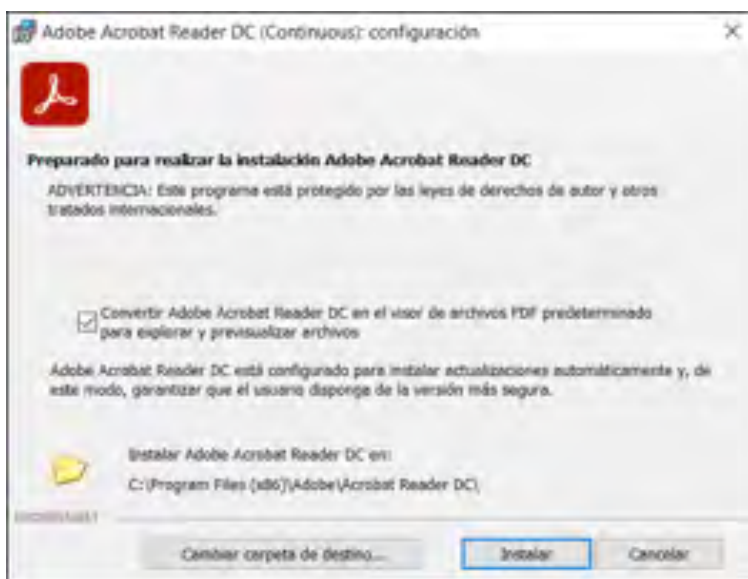
The installation paths for Acrobat Reader DC are described below:

- ▶ **Installation path on Windows (32bits)**
C:\Program Files (x86)\Adobe\Acrobat Reader DC\
- ▶ **Installation path on Windows (64bits)**
C:\Program Files\Adobe\Acrobat Reader DC\
- ▶ **Registration path**
HKCU\Software\Adobe\Acrobat Reader\DC\
- ▶ **Application data path**
%Appdata%\Roaming\Adobe\Acrobat\DC\

For continuous monitoring, all the services are visible

For continuous monitoring, all the services are visible. Free Adobe Document Cloud services are functional by default, and paid services require an upgrade or purchase.

For the Acrobat DC Enterprise version, the default setting of Adobe Acrobat Reader DC as the default PDF viewer is checked during the installation process.



NOTE:

It is possible to customise the path where the programme installation takes place in the programme installation process.

3.5. Downloading and installing Reader

3.5.1. Acrobat Reader DC (Enterprise)

Via the following URL:

<https://get.adobe.com/es/reader/enterprise/>

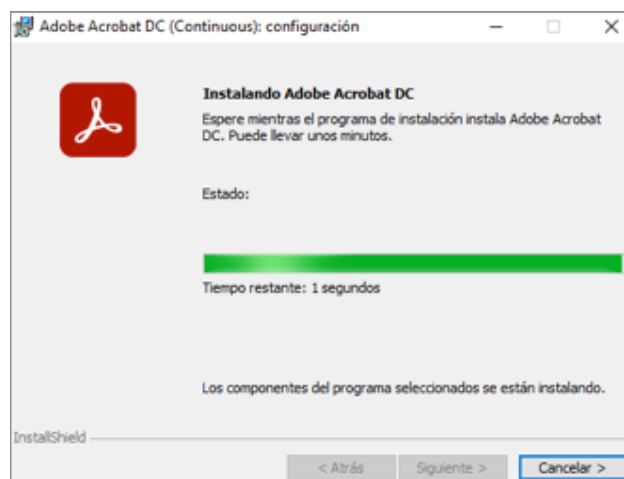
All versions of Adobe Acrobat Reader DC available for download at this link use continuous tracking.

DESCRIPTION

▶ In this window we will select the operating system in which we will install this download "**Step 1**", the language "**Step 2**" and finally the version "**Step 3**". Next, click on the "**Download now**" button to start downloading the programme. Once this step has been completed, double click on the installation file and wait until the installation process has finished.

▶ The installation file you download will be used to install or update the version of Acrobat Reader.

▶ Restart the system and you are ready to use the programme.



3. Installing and bashing Adobe Reader DC continuous track on Windows

3.5.2. Acrobat Reader DC (individuals)

Via the following URL:

<https://get.adobe.com/es/reader/>

Adobe Acrobat Reader DC is installed directly on your computer. Internet is required to complete the authorisation process at first launch and every 30 days in order to validate your subscription.

DESCRIPTION

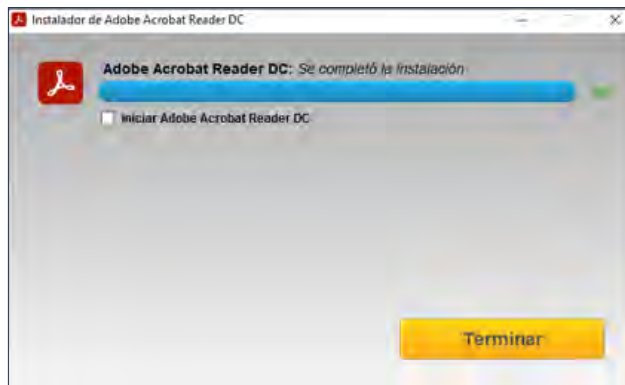
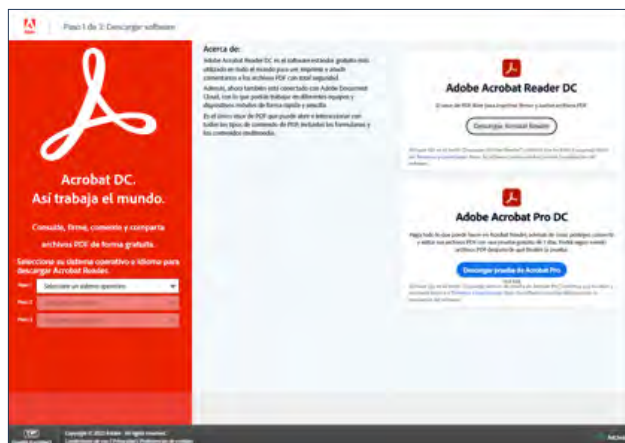
In this window we will select the operating system in which we will install this download "**Step 1**", the language "**Step 2**" and finally the version "**Step 3**". Next, click on the "**Download Acrobat Reader**" button to start downloading the Adobe Acrobat installation file, called "reader[xxx]_install.exe".

Once this step has been completed, double-click on the installation file to complete the installation.

NOTE:

The installation of Acrobat Reader DC is a two-step process: you download the installer and then install Reader.

Click **Finish** and **reboot** the system. You are now ready to use the programme.



3.6. Apply security values

The following is a step-by-step description of how to add the .admx and .adml files and security settings to bastion Adobe Reader DC on a Windows machine.

3.6.1. Windows client

In this example, it is assumed that the computer on which the scripts are to be executed has the Windows operating system and Adobe Reader DC installed.

| DESCRIPTION | |
|---|--|
| 1. | Log in with a user who has administrator privileges and is a member of the "Shell Users" group on the machine where you want to run the scripts. |
| 2. | Copy the files and folders accompanying this guide to the "C:\Scripts" directory of the equipment. |
| 3. | Make sure that at least the following files have been copied to the directory "C:\Scripts": <ul style="list-style-type: none">– GP Report– GPOs– PolicyDefinitions– Scripts_local |
| 4. | Then go to the folder "C:\Scripts_local" and run the file "Import ADMX - Install GPO.bat" as administrator (Run as administrator option). |
| 5. | The Administrative Templates will be added correctly and the GPO values imported. |
| 6. | When the execution is finished, press a key again to close the window. |
| 7. | Reboot the system. |
| NOTE: Importing Local Group Policy settings from the GPO backup contained in the Scripts folder is done with the free LGPO.exe tool which is a command-line utility for automating Local Group Policy management and is part of the Microsoft Security Compliance Toolkit. Download URL: https://www.microsoft.com/download/details.aspx?id=55319 | |

3. Installing and bashing Adobe Reader DC continuous track on Windows

3.6.2. Windows server, how to create and manage the central repository for group policy administrative templates

The following describes how to use the .admx and .adml files to create and manage registry-based policy settings in Windows, in addition to how to use the central store to store and replicate the Adobe Reader DC Group Policy files, which accompany this guide, in a domain environment.

THE CENTRAL WAREHOUSE

To take advantage of .admx files, you must create a Central store in the SYSVOL folder on a domain controller. The Central store is a file location that is protected by the Group Policy tools. The Group Policy tools use any .admx files that are in the Central store. Later, the files found in the Central store are replicated to all domain controllers in the domain.

To create a Central store for .admx and .adml files, create a folder named PolicyDefinitions in the following location:

\\FQDN\SYSVOL\FQDN\policies

NOTE:

FQDN is a fully qualified domain name.

For example, to create a Central store for the contoso.com domain, create a PolicyDefinitions folder in the following location:

\\contoso.com\SYSVOL\contoso.com\policies

Copy all files from the PolicyDefinitions folder, which accompanies this guide, to the PolicyDefinitions folder on the domain controller. The PolicyDefinitions folder, which accompanies this guide, stores the .admx and .adml files for the Spanish (es-ES) language.

Now if we open a GPMC and edit an existing policy, we will see that the new type of template that we have enabled with the PolicyDefinitions directory appears in the administrative templates, and also in our language.

In the GPO folder of this guide you will find a backup GPO with the security settings.



3.7. Register values

The following are the security modifications implemented at registry level in the security enhancement process set out in section "3.6. Apply security settings".

| | |
|---|---|
| <p>▶ Adobe Reader DC should prevent the opening of non-PDF and non-FDF files</p> | <p>Attachments represent a potential security risk because they may contain malicious content, open other dangerous files or launch applications.</p> <p>Files with extension .bin, .exe, .bat, etc. will be recognised as threats.</p> <p>This function prevents users from opening or launching file types other than PDF or FDF and disables the menu option.</p> <p>The value of "iFileAttachmentPerms" must be set to "1" and the type set to "REG_DWORD".</p> |
| <p>CHECK</p> | <p>GUI Path: Edit> Preferences> Trust Manager> In the section 'PDF file attachments'> Check "Allow opening non-PDF files with external applications" should show the checkbox unchecked and greyed out (locked).</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "iFileAttachmentPerms"</p> |





3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|--|
|  Adobe Reader DC must block Flash content | <p>Adobe Reader and Acrobat stopped shipping with a dedicated Flash player in version 9.5.1. Since then, rendering Flash content in a PDF requires that the Flash Player is already on the user's machine.</p> <p>This strategy simplifies Acrobat and Reader deployments by reducing the number of future updates required in the event of a security issue.</p> <p>Flash content can be embedded in PDFs and could be used to install malicious software on a user's computer.</p> <p>The value of "bEnableFlash" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bEnableFlash" |
|  Adobe Reader DC must disable all service access to Document Cloud Services | <p>By default, Adobe's online services are tightly integrated with Adobe Reader DC.</p> <p>With Adobe Document Cloud integration, disabling this feature avoids the risk of additional attack vectors.</p> <p>Within Adobe Reader DC, Adobe Cloud resources require a paid subscription for each service.</p> <p>The value of "bToggleAdobeDocumentServices" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices" /v "bToggleAdobeDocumentServices" |
| | NOTE: The key name "cServices" is not created by default in the Adobe Reader DC installation and must be created. |



3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|--|---|
| ▶ Adobe Reader DC must enable Enhanced Security in a separate application | <p>PDF files have evolved from static pages to complex documents with features such as interactive forms, multimedia content, scripting and other capabilities.</p> <p>These features make PDF files vulnerable to malicious scripts or actions that can damage the system or steal data.</p> <p>The enhanced security feature protects the system against these threats by blocking or selectively allowing actions for trusted locations and files.</p> <p>Enhanced security determines whether a PDF is viewed within a standalone application. A threat to Adobe Reader DC users is opening a PDF file containing malicious executable content.</p> <p>Enhanced security "hardens" the application against risky actions such as preventing access to multiple domains, prohibiting data and script injection, blocking script access to XObjects, silent printing and high privilege JavaScript execution.</p> <p>The value of "bEnhancedSecurityStandalone" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Security (Enhanced)> In the 'Enhanced Security' section > The 'Enable Enhanced Security' checkbox is checked and unchecked (locked).</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bEnhancedSecurityStandalone"</p> |
| ▶ Adobe Reader DC must disable third-party web connectors | <p>When third party web connectors are disabled, it prevents the configuration of Adobe Reader DC access to third party services for file storage.</p> <p>The value of "bToggleWebConnectors" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices" /v "bToggleWebConnectors"</p> <p>NOTE: The key name "cServices" is not created by default in the Adobe Reader DC installation and must be created.</p> |



3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|---|
|  Adobe Reader DC must disable cloud synchronisation | <p>By default, Adobe's online services are tightly integrated with Adobe Reader DC.</p> <p>When Adobe Cloud synchronisation is disabled, it prevents synchronisation of desktop preferences on devices where the user is signed in with an Adobe ID (including phones).</p> <p>The value of "bTogglePrefsSync" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices" /v "bTogglePrefsSync"</p> <p>NOTE: The key name "cServices" is not created by default in the Adobe Reader DC installation and must be created</p> |
|  Adobe Reader DC must enable FIPS mode | <p>The use of weak or untested encryption algorithms undermines the purposes of using encryption to protect data.</p> <p>The application must implement cryptographic modules that comply with the highest standards approved by entities, as this ensures that they have been tested and validated.</p> <p>The value of "bFIPSMODE" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\AVGeneral" /v "bFIPSMODE"</p> |



3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|--|--|
|  Adobe Reader DC must disable access to Webmail | <p>When Webmail is disabled, the user cannot set up a webmail account to send an open PDF document as an attachment.</p> <p>Users must have the ability to send documents as Microsoft Outlook attachments.</p> <p>The difference is that Outlook must be configured by the administrator on the local machine.</p> <p>The value of "bDisableWebmail" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cWebmailProfiles" /v "bDisableWebmail"</p> <p>NOTE: El nombre de la clave "cWebmailProfiles" no se crea de forma predeterminada en la instalación de Adobe Reader DC y debe crearse</p> |
|  Adobe Reader DC must disable the ability to elevate (trust) certified documents as a privileged location | <p>Privileged locations allow the user to selectively trust files, folders and hosts to bypass some security restrictions, such as enhanced security and protected view.</p> <p>By default, the user can create privileged locations through the GUI.</p> <p>Disabling certified documents disables and blocks the end-user's ability to elevate certified documents as a privileged location.</p> <p>The value of "bEnableCertificateBasedTrust" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Security (Enhanced)> In the 'Privileged Location' section, verify that the 'Automatically trust documents with a valid certification' option is disabled and greyed out (locked)..</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bEnableCertificateBasedTrust"</p> |



3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|---|
|  Adobe Reader DC should block websites | <p>Clicking on any link to the Internet represents a potential security risk.</p> <p>Malicious websites can transfer harmful content or collect data silently.</p> <p>Acrobat Reader documents can connect to websites that may pose a potential threat to systems and that functionality should be blocked.</p> <p>However, trusted PDF document workflows can benefit from leveraging legitimate access to websites with minimal risk.</p> <p>Therefore, it may approve access to websites and accept the risk if the access provides a benefit and is a trusted site or the risk associated with accessing the site has been mitigated.</p> <p>The value of "iURLPerms" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>Ruta GUI: Edit> Preferences> Trust Manager> In the section "Internet access from PDF files outside the web browser"> Select the option "Change settings"> In the "PDF files can connect to websites to share or get information" section> Verify the radio button "Block PDF files access to all websites" is selected and disabled (locked).</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms" /v "iURLPerms"</p> |
|  Adobe Reader DC must enable protected mode | <p>A threat to Adobe Reader DC users is opening a PDF file containing malicious executable content.</p> <p>Sandboxing is a technique for creating an isolated execution environment, which allows untrusted programs to run.</p> <p>In the context of Adobe Reader, an "untrusted program" is any PDF and the processes it invokes.</p> <p>When sandboxing is enabled, Reader assumes that all PDF files are potentially malicious and limits any processing by invoking it.</p> <p>This isolation of PDF files reduces the risk of security breaches in areas outside the sandbox.</p> <p>The value of "bProtectedMode" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit>Preferences> Security (Enhanced)> Test Site Protections> Enable Protected Mode at startup.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bProtectedMode"</p> |




3. Installing and basing Adobe Reader DC continuous track on Windows

| | |
|---|--|
|  Adobe Reader DC must enable protected view | <p>It is essentially a read-only mode. This function is based on sandbox technology.</p> <p>In Reader, Protected View is only supported when "Protected Mode" is enabled. If an HKCU or HKLM Protected Mode registry key is set to 0 (off), Protected View cannot be enabled.</p> <p>The value of "iProtectedView" must be set to "2" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Security (Enhanced)> Protected View (All Files).</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "iProtectedView"</p> |
|  Adobe Reader DC must enable Enhanced Security in a browser | <p>PDF files have evolved from static pages to complex documents with features such as interactive forms, multimedia content, scripting and other capabilities.</p> <p>Enhanced security blocks specific behaviours such as: data injection, script injection, silent printing, web links (if not allowed by Trust Manager settings), cross-domain access and access to external streams.</p> <p>The value of "bEnhancedSecurityInBrowser" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Security (Enhanced)> Enhanced Security > Enable Enhanced Security.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bEnhancedSecurityInBrowser"</p> |



3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|--|--|
|  Adobe Reader DC should block access to unknown websites | <p>Because accessing the Internet is a potential security risk, clicking on any unknown website link to the Internet represents a potential security risk. Malicious websites can transfer harmful content or silently collect data.</p> <p>The value of "iUnknownURLPerms" must be set to "3" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Trust Manager> Internet Access from PDF Files outside Web Browser> Change Settings> Block PDF files access to all websites.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cDefaultLaunchURLPerms" /v "iUnknownURLPerms"</p> |
|  Adobe Reader DC must disable Online SharePoint Access | <p>Desactiva las características de integración de SharePoint y Office 365. Controla la capacidad de la aplicación para detectar que un archivo proviene de un servidor de SharePoint. Deshabilita la solicitud de extracción y elimina los elementos del menú específicos de SharePoint.</p> <p>El valor de "bDisableSharePointFeatures" debe estar establecido en "1" y el tipo configurado como "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cSharePoint" /v "bDisableSharePointFeatures"</p> <p>NOTE: The key name "cSharePoint" is not created by default in the Adobe Reader DC installation and must be created.</p> |

3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|--|---|
|  Adobe Reader DC should disable the ability to elevate IE trusts to privileged locations | <p>Privileged locations allow the user to selectively trust files, folders and hosts to bypass some security restrictions, such as enhanced security and protected view.</p> <p>Disabling IE trust in privileged locations disables and blocks the end-user's ability to treat IE trusted sites as a privileged location.</p> <p>The value of "bDisableTrustedSites" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Security (Enhanced)> Privileged Locations > Add Host. This option should be greyed out.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bDisableTrustedSites"</p> |
|  Adobe Reader DC should disable the ability to add trusted files and folders | <p>Disables trusted folders and files and prevents users from specifying a privileged location for directories.</p> <p>The value of "bDisableTrustedFolders" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit > Preferences > Security (Enhanced) > Privileged Locations > Add Folder Path. This option should be greyed out.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bDisableTrustedFolders"</p> |
|  Adobe Reader DC must disable the ability to specify host-based privileged locations | <p>Disables and blocks the ability to specify host-based privileged locations.</p> <p>The value of "bDisableOSTrustedSites" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit > Preferences > Security (Enhanced) > Privileged Locations > Automatically trust sites in my Win OS security zones. This option must be disabled.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bDisableOSTrustedSites"</p> |

3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|--|
|  Adobe Reader DC must disable the ability to change the default driver | <p>Disables the ability to change the specific default driver (PDF viewer).</p> <p>The value of "bDisablePDFHandlerSwitching" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit > Preferences> General> Select as default PDF driver. This option should be greyed out</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bDisablePDFHandlerSwitching"</p> |
|  Adobe Reader DC must disable the Adobe Send and Track Add-in for Outlook | <p>When enabled, an Adobe Send and Track button appears in Outlook when composing an email.</p> <p>Allows large files to be sent as public links via Outlook.</p> <p>Attachments are uploaded to Adobe Document Cloud and public links to the files are inserted in the body of the email.</p> <p>Recipients can click on the link to preview the file in a browser window and can download the file if necessary.</p> <p>The value of "bAdobeSendPluginToggle" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices" /v "bAdobeSendPluginToggle"</p> <p>NOTE: The "cCloud" key name is not created by default in the Adobe Reader DC installation and must be created.</p> |

3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|---|
| ▶ Adobe Reader DC must disable Adobe Send for Signature (Adobe Sign) | <p>Deactivate Adobe Send for Signature (Adobe Sign).</p> <p>The Adobe Document Cloud signature service allows users to send documents online to be signed from any location or device.</p> <p>Signed documents are stored in the Adobe cloud.</p> <p>The Adobe Document Cloud signature service works on a subscription basis.</p> <p>When Adobe Send for Signature is disabled, users will not be able to use the Adobe Document Cloud signature feature.</p> <p>The value of "bToggleAdobeSign" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices" /v "bToggleAdobeSign"</p> <p>NOTE: The "cCloud" key name is not created by default in the Adobe Reader DC installation and must be created.</p> |
| ▶ Adobe Reader DC must disable Adobe's repair installation | <p>When the Repair Installation is disabled, the user does not have the option (Help Menu) or functionality to repair an Adobe Reader DC installation.</p> <p>The value of "DisableMaintenance" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Help> Repair installation. This option should be greyed out.</p> <p>For 32 bits: REG QUERY "HKEY_LOCAL_MACHINE\Software\Adobe\Acrobat Reader\DC\Installer" /v "DisableMaintenance"</p> <p>For 64 bits: REG QUERY "HKEY_LOCAL_MACHINE\Software\Wow6432Node\Adobe\Acrobat Reader\DC\Installer" /v "DisableMaintenance"</p> |




3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|---|
|  Adobe Reader DC must disable the periodic uploading of Adobe certificates | <p>Specifies whether trusted certificates can be downloaded periodically from Adobe.</p> <p>The value of "bLoadSettingsFromURL" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit> Preferences> Trust Manager> Adobe Approved Trust List (AATL) Automatic Updates> Load trusted certificates from an Adobe AATL server. The box must be unchecked.</p> <p>REG QUERY "HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cDigSig\cAdobeDownload" /v "bLoadSettingsFromURL"</p> <p>NOTE: The key names "cDigSig" and "cAdobeDownload" are not created by default in the Adobe Reader DC installation and must be created.</p> |
|  Adobe Reader DC should disable the periodic uploading of European certificates | <p>Specifies whether trusted certificates can be downloaded periodically from Adobe.</p> <p>The value of "bLoadSettingsFromURL" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit > Preferences> Trust Manager> European Lists Automatic Updates (EUTL)> Load trusted certificates from an Adobe EUTL server. The box must not be checked.</p> <p>REG QUERY "HKEY_CURRENT_USER\Software\Adobe\Acrobat Reader\DC\Security\cDigSig\cEUTLDownload" /v "bLoadSettingsFromURL"</p> <p>NOTE: The key names "cDigSig" and "cEUTLDownload" are not created by default in the Adobe Reader DC installation and must be created.</p> |
|  Adobe Reader DC must disable Acrobat Upsell | <p>For DC products, disable messages that encourage the user to upgrade the product. For example, Reader users can purchase additional tools and features.</p> <p>The value of "bLoadSettingsFromURL" must be set to "1" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\Software\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bAcroSuppressUpsell"</p> |

3. Installing and bashing Adobe Reader DC continuous track on Windows

| | |
|---|---|
|  Adobe Reader DC must disable the Adobe welcome screen | <p>Disables the welcome screen when starting the application.</p> <p>The value of "bShowWelcomeScreen" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | <p>GUI Path: Edit > Preferences> General> Application startup> Show splash screen. The box must be unchecked.</p> <p>REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cWelcomeScreen" /v "bShowWelcomeScreen"</p> <p>NOTE: The key name "cWelcomeScreen" is not created by default in the Adobe Reader DC installation and must be created.</p> |
|  Adobe Reader DC must disable both updates to the product's web plug-in components and all services | <p>By default, Adobe's online services are seamlessly integrated into Adobe Reader DC.</p> <p>Disabling the service updates disables the updates to the product's web plug-in components and all services without exception, including any online login screens.</p> <p>The value of "bUpdater" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown\cServices" /v "bUpdater"</p> <p>NOTE: The key name "cServices" is not created by default in the Adobe Reader DC installation and must be created.</p> |
|  Adobe Reader DC should disable product updates | <p>Disable product updates.</p> <p>The value of "bUpdater" must be set to "0" and the type set to "REG_DWORD".</p> |
| CHECK | <p>REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\DC\FeatureLockDown" /v "bUpdater"</p> |

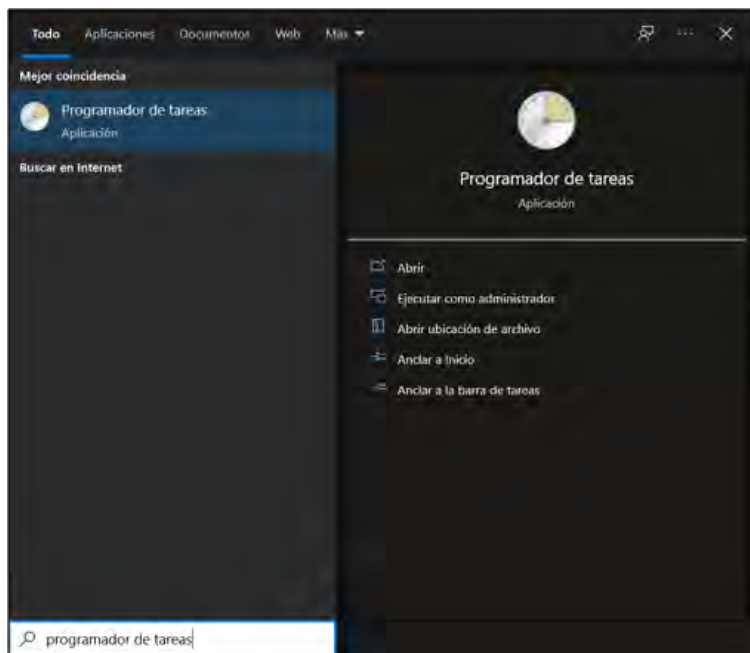
3. Installing and bashing Adobe Reader DC continuous track on Windows

| Additional registry values | |
|--|--|
|  Player options | <p>Apple no longer provides security updates for legacy QuickTime for Windows software, making this software vulnerable to exploitation. Therefore, to protect Reader, Adobe has also removed support for QuickTime on Windows. Reader DC now uses the built-in Windows video player to play legacy QuickTime videos, which are the videos embedded in PDF documents created with Acrobat 9 and earlier. If this option is not selected and QuickTime Player is not available, Windows uses its built-in player.</p> <p>GUI Path: Edit> Preferences> Multimedia (legacy)> under "Player Options" verify that "Do not use QuickTime Player for media items" is checked.</p> |
|  JavaScript | <p>Allows you to adjust the behaviour of the application so that JavaScript runs at the desired security level. This allows limiting the application's access to JavaScript APIs and isolates workflows that do not require JavaScript APIs.</p> <p>Uncheck this option to disable JavaScript completely or restrict JavaScript via APIs.</p> <p>GUI Path: Edit> Preferences> JavaScript> under "JavaScript" check that "Enable Javascript for Acrobat" is unchecked.</p> |
|  Documents in the list of recent files | <p>The recent files list provides shortcuts to your recently opened files. This is a lack of privacy if you share the device with anyone.</p> <p>If we reduce this option to zero, the recent list is disabled.</p> <p>GUI Path: Edit> Preferences> Documents> under "Open settings" verify that "Documents in recent files list:" is set to zero (0).</p> |

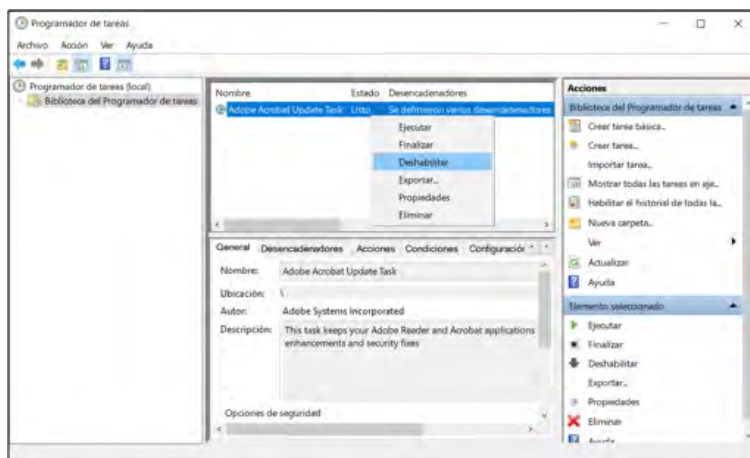
3.8. Disable the Adobe Acrobat update task

The first step to disable the automatic update in Adobe Reader is to disable the 'Adobe Acrobat Update Task' in the Task Scheduler. To do this:

- ▶ In the search box, type:
task scheduler
- ▶ Open Task Scheduler and Run as administrator



- ▶ Click Task Scheduling Library on the left, and then in the right pane, right-click the **Adobe Acrobat update** task and select **Disable**.



3.9. Disable “AdobeARMservice” service

The following is a step-by-step description of how to set up the "Adobe-ARMservice" on a standalone Windows machine.

In this example, it is assumed that the computer on which this functionality is to be disabled has the Windows operating system and Adobe Reader DC installed.

| DESCRIPTION | |
|---|---|
| 1. | Log in with a user who has administrator privileges and is a member of the "Shell Users" group on the machine where you want to disable "AdobeARMservice". |
| 2. | Copy the files and folders accompanying this guide to the "C:\scripts" directory on your computer. |
| 3. | Make sure that at least the following files have been copied to the directory "C:\Scripts\Scripts_local": <ul style="list-style-type: none">– AdobeARMservice.bat– AdobeARMservice.inf |
| 4. | Then go to the folder "C:\Scripts_local" and run the file "AdobeARMservice.bat" as administrator (Run as administrator option). |
| 5. | You will need to re-enter the user credentials with administrator privileges. |
| 6. | In the pop-up window, press a key to start the execution of the script. When the execution is finished, press a key again to close the window. |
| 7. | The "AdobeARMservice" service has been successfully deactivated. |
| NOTE: For domain-joined client machines, it is recommended to disable the "AdobeARMservice" service via group policies set in the domain. | |

4. Checklist (assessment)

| CRITICALITY | VERIFICATION |
|-------------|---|
| High | Adobe Reader DC must have the latest security-related software updates installed. |
| Medium | Adobe Reader DC must disable the update service " AdobeARMservice ". |
| Medium | Adobe Reader DC should avoid opening files other than PDF or FDF files. |
| Medium | Adobe Reader DC must block Flash content. |
| Medium | Adobe Reader DC must disable all service access to Document Cloud Services . |
| Medium | Adobe Reader DC must enable Enhanced Security in a separate application. |
| Medium | Adobe Reader DC must disable third-party web connectors. |
| Medium | Adobe Reader DC must disable cloud synchronisation. |
| Medium | Adobe Reader DC must enable FIPS mode. |
| Medium | Adobe Reader DC must disable access to webmail . |
| Medium | Adobe Reader DC must disable the ability to elevate (trust) certified documents as a privileged location. |
| Medium | Adobe Reader DC should block websites. |
| Medium | Adobe Reader DC must enable Protected View. |

4. Checklist (assessment)

| CRITICALITY | VERIFICATION |
|-------------|--|
| Medium | Adobe Reader DC must enable protected mode. |
| Medium | Adobe Reader DC must enable Enhanced Security in a browser. |
| Medium | Adobe Reader DC should block access to unknown websites. |
| Medium | Adobe Reader DC must disable Online SharePoint Access . |
| Medium | Adobe Reader DC should disable the ability to elevate IE trusts to privileged locations. |
| Medium | Adobe Reader DC should disable the ability to add trusted files and folders. |
| Medium | Adobe Reader DC must disable the ability to specify host-based privileged locations. |
| Low | Adobe Reader DC must disable the ability to change the default driver. |
| Low | Adobe Reader DC must disable the Adobe Send and Track Add-in for Outlook. |
| Low | Adobe Reader DC must disable Adobe Send for Signature . |
| Low | Adobe Reader DC must disable Adobe's repair installation. |
| Low | Adobe Reader DC must disable the periodic uploading of Adobe certificates. |
| Low | Adobe Reader DC should disable the periodic uploading of European certificates. |
| Low | Adobe Reader DC must disable Acrobat Upsell . |
| Low | Adobe Reader DC must disable the Adobe welcome screen. |
| Low | Adobe Reader DC must disable service updates. |

5. Decalogue of recommendations

Security Decalogue for Acrobat Reader DC

- 1 Always use the latest version of Adobe
- 2 It is advisable to review any security-related features of the software, as they provide a stronger defence against attacks.
- 3 It is recommended to lock the user interface so that the end-user cannot change the settings.
- 4 Metadata cleaning is recommended when pdf files are publicly accessible.
- 5 It is recommended to use Adobe Reader DC only for opening PDF or FDF files.
- 6 It is recommended to use a digital certificate to sign PDF documents in order to guarantee authorship against possible manipulations or modifications by third parties.
- 7 It is recommended not to use third-party plugins.
- 8 It is recommended to block links to the internet in PDF files.
- 9 It is recommended to enable protected mode and view.
- 10 It is recommended to block any kind of Internet connection from PDF files.

ANNEX. Secure configuration scripts

To facilitate the implementation of the Acrobat Reader DC security patch, a script folder is included in this document, which contains the files necessary for the program's bastioning.

The purpose of scripts is to execute scripts automatically, mitigating as far as possible failures caused when basing a specific system or programme.

The files or folders included in the "**Scripts**" folder are listed below.

| | |
|-------------------|---|
| GP Report | <ul style="list-style-type: none">▶ Adobe Reader DC Continuous - team.htm▶ Adobe Reader DC Continuous - user.htm |
| GPOs | <ul style="list-style-type: none">▶ {5FDCB222-F465-4C7C-864B-E5EE4E8BFA09}▶ {CD465C95-EA48-4901-A8F1-41A65B64ECFA} |
| PolicyDefinitions | <ul style="list-style-type: none">▶ en-EN<ul style="list-style-type: none">• AcrobatReaderDC.adml▶ AcrobatReaderDC.admx |
| Scripts_local | <ul style="list-style-type: none">▶ Tools<ul style="list-style-type: none">• LGPO.exe▶ Import ADMX - Install GPO.bat▶ Import ADMX - Install GPO.ps1▶ AdobeARMservice.bat▶ AdobeARMservice.ps1 |



www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

