Adobe Reader 7: Minimizing Exposure of Personal Information on Public Computers

CONTENTS

Introduction

When Adobe® Reader® 7 is used on a public computer, it is possible for one user's personal information to be seen by other users. This document describes methods system administrators can use to help minimize the amount of sensitive information that might be exposed in that situation.

The methods described in this document include setting user preferences, editing the registry to lock features, and using a JavaScript script to hide menu items. Some systems will not require all procedures described in this document; you will need to choose the methods appropriate for your system and situation. In addition, administrators should observe all relevant security practices recommended by Microsoft® for using Windows® on public computers.

The information presented in this document was written for, and tested with, Adobe Reader 7.0.8 on Windows. However, it should be generally applicable to older versions of Reader on Windows, as well as versions on other operating systems.

NOTE: Several procedures in this document involve editing the Windows registry, which can cause significant changes to a system if not done correctly. Registry editing should only be done by a qualified individual, and the registry and system should always be backed up prior to registry editing.

Intended Audience

This document is for system administrators who are familiar with the installation and management of a multi-user Windows system. It assumes that you have a basic understanding of Adobe Reader and the use of JavaScript scripting for PDF documents.

Other Options

This document describes detailed methods to minimize exposure of personal information. However, there are two options available that can help you to install and manage Reader's operation on public kiosk systems:

InstallShield Tuner 7.0 for Adobe Acrobat. A free utility that allows system administrators to customize the Adobe Reader installer. The InstallShield Tuner allows you to customize installations to set preferences and to create or edit registry keys. It is intended mainly for larger-scale enterprise deployments, but it can also be used by smaller organizations. While it initially requires more learning and set-up time, it can customize the installation and standardize the operation of Reader for an entire organization, thus reducing problems and saving time in the future. For more information, see the link for the InstallShield Tuner in "References" on page 21.

Off-the-Shelf Kiosk Management Tools. Some administrators may prefer to use off-the-shelf software tools for managing public kiosk systems. Using those tools, you can use standard methods to save and restore registry settings and JavaScript files, set preferences, and to delete files with persistent data—using the information described in this document.

Basic Methods

This section discusses the methods recommended for Adobe Reader 7 to ensure minimal exposure of personal information.

Setting Preferences. Adobe Reader preferences can be set by a system administrator, or by using the InstallShield Tuner utility (see "InstallShield Tuner 7.0 for Adobe Acrobat.").

It is recommended that administrators set the preferences, and then hide the Preferences menu item using folder-level JavaScript scripts (see below). That will prevent most users from changing the settings, but will not prevent a user from using the keyboard shortcut (Ctrl-k) to invoke the Preferences window.

For the features discussed in this document, the only one that has a keyboard shortcut is the Preferences window, which can be opened using Ctrl-k.

Adding JavaScript Scripts. JavaScript scripts can be used to hide Reader menu items and to set some preferences.

To install a script, the selected code is put into a text file with a "`.js`" extension, and the file is placed in the application's JavaScripts folder at:

```
C:\Program Files\Adobe\Acrobat 7.0\Reader\JavaScripts
```

For Reader 7.0, the script will be executed either when the application is first launched, or after the first JavaScript script is executed. The script files in that folder will be *read-only*, so users will be able to see the scripts, but they will not be able edit the file. See the *JavaScript for Acrobat API Reference* for more information.

When a menu item is hidden, it is not fully disabled. The associated function may be invoked in the following ways:

- If there is a keyboard shortcut for the feature. The only feature discussed in this document that has a keyboard shortcut is the Preferences window (Ctrl-k). That means that a knowledgeable user can always access and change their preference settings.
- If a document script invokes the feature directly, such as: `app.mailMsg` or `app.mailForm`, or by executing a menu item, such as: `app.execMenuItem("AcroSendMail:SendMail")`.

  Note that when `app.execMenuItem` is used, Reader limits execution to menu items that are not likely to be a security risk.

All JavaScript code shown in this document is listed in the section "Collected Scripts" on page 20.

Editing the Registry. If the user is logged in as User or Guest, or their account is set to use the Mandatory User Profile, in most cases the user will not be able to edit the registry (unless they are granted certain privileges when using the Mandatory User Profile). Therefore, protections set in the registry by the administrator generally cannot be changed by the user.

Reader supports a *lockdown* feature, controlled by registry entries, which can be used to lock some security features, such as the first two listed in Table 1 below. Registry entries can also used to enforce the preferred behavior of other features, such as the last two listed in Table 1.

TABLE 1 Feature functions controlled by registry entries

Feature	Lockdown	Purpose of registry editing	Reference
Forms: Auto-complete	✓	Turn off Auto-complete feature	See "Forms" on page 14
URL Trust Manager	✓	Prevent saving URLs	See "URL Trust Manager" on page 19
Digital Signatures		Prevent user from creating self-signed digital IDs	See "Digital Signatures" on page 10
Policy Server Access		Prevent Adobe LiveCycle policy server from caching user password	See "Policy Server Access" on page 14

NOTE: Some registry entries will only appear if certain application features are excercised. On a Windows system, a registry entry for most entries will only exist if the value is not set to the default value.

Overview of Possible Information Exposure

Table 2, "Minimizing Information Exposure for Adobe Reader," provides an overview of possible information exposure, and the sections that follow discuss each issue in more depth.

Not all issues will apply to all deployments, and administrators need to decide which ones are appropriate for their system. For example, it matters whether users will have access to Reader enabled PDF files, which are PDF files that have been granted higher privileges by either Acrobat Professional or Adobe LiveCycle Policy Server®. If the user can access PDF files either internally or from the Internet, then the features related to enabled PDFs (shown below) must be considered. However, if it is a closed system that only allows limited user functions, then features and actions related to enabled PDFs can be ignored.

IMPORTANT: *Features that are dependent on Reader enabled PDF are shown with a check mark in the second column of Table 2.*

Table 2 Minimizing Information Exposure for Adobe Reader

Feature	Only for Reader Enabled PDF?	Description	JavaScript	RegEdit	Preferences	Recommended Method for Minimizing Exposure
Email		Menu item and toolbar icon can be used to attach PDF to an Email message	✓			Hide Email menu item and toolbar icon. See "Adding JavaScript Scripts" on page 2.
Send for Review		Reader's Tracker may save information about PDF reviews.	✓			Hide the menu item for Review Tracker using JavaScript. See Adding JavaScript Scripts for more information. No keyboard shortcut.
Spell Checking Dictionary		Words added to spell checking dictionary could reveal sensitive information.	✓			Use JavaScript script to hide the Spell Checking menu item.
Digital Signatures	✓	User can create a self-sign digital ID; they can sign and save to local computer. Workflow items can persist.	✓	✓		1. Edit registry to prevent creation of digital IDs. See "Editing the Registry" on page 3. 2. Hide digital signature menu items using JavaScript. See "Adding JavaScript Scripts" on page 2. There is no keyboard shortcut for this feature.
Trusted Identities	✓	A digital ID can be seen by another user when it is added to Trusted Identity list.	✓			Hide menu item using JavaScript. See "Adding JavaScript Scripts" on page 2. No keyboard shortcut for Trusted Identities.
Policy Server Access	✓	For an enabled PDF, user's password could be cached.		✓		Edit registry to turn off caching. See "Editing the Registry" on page 3.
Forms	✓	User can allow PDF form data to be retained.	✓	✓	✓	1. Turn off Auto-complete feature *Optional:* 2. Hide Preferences using JavaScript. 3. Edit registry to disable Auto-Complete Keyboard shortcut can be used to access the Preferences window.
Auto-save File Changes		User can Auto-save file edits to a temp file; user chooses time interval.	✓		✓	Increase time setting to 99 minutes, and hide Preferences menu item. See "Setting Preferences" on page 2 for more information.

Feature	Only for Reader Enabled PDF?	Description *(Continued)*	JavaScript	RegEdit	Preferences	Recommended Method for Minimizing Exposure
Search: Cache Index Information		Optional caching of file search results. Cache file persists and can be seen by all users, but file format is proprietary.	✓		✓	Turn off Fast Find; and use JavaScript to hide Preferences menu. See "Setting Preferences" and "Adding JavaScript Scripts" on page 2 for more information. Keyboard shortcut can be used to access Preferences menu.
Recently Opened Files		Reader maintains a list of recently opened files.	✓		✓	1. Set the value to 1. See ""Setting Preferences" on page 2. 2. Hide Preferences menu item; see "Adding JavaScript Scripts" on page 2". Keyboard shortcut can be used to access Preferences menu.
URL Trust Manager		User can add URLs for Web sites allowed or blocked for sending or receiving of data	✓		✓	1. Edit the registry to lock the URL Trust Manager.

Details for each issue shown in the above table are described in greater detail in the following sections.

General Precautions

User Login Accounts. Users' accounts should be set so users can only login as either User, or Guest. Also, a Mandatory User Profile can be used to ensure that changes in the system settings and data are removed from a system every time a user logs off. With a User or Guest account, the user can edit settings in the Current User section of the registry, but cannot edit the Local Machine settings.

Preferences Menu. The Preferences menu item in the Edit menu can be hidden using the following folder-level JavaScript line item:

```
app.hideMenuItem("GeneralPrefs");
```

This is optional, but it is a good general precaution to prevent users from changing preferences, and is specifically recommended for a number of the recommended methods described in this document.

Data saved by Reader. Reader, like most Windows' applications, may write data to the user's application data folder. For example, there are two files, `glob.js` and `glob.settings.js`, which may be created and used by a script in a document, or by Reader itself. The recommended practice is to create a batch file to periodically delete those files in the Reader area of Application Data:

```
C:\Documents and Settings\Adobe\Acrobat 7.0\Reader\JavaScripts\
```

Methods for Minimizing Exposure of Personal Information

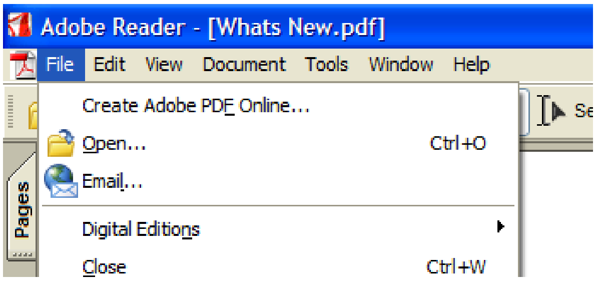
This section describes known issues related to information exposure and describes the recommended procedure to minimize the risk.

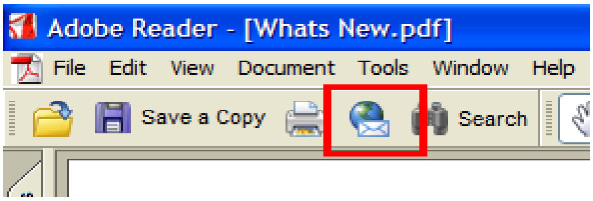
Email

Feature Reader can access the user's default Email application (via MAPI) and attach a PDF to an outgoing Email. This is only relevant if a local default MAPI Email client exists.

Possible Information Exposure It may not be appropriate for a public computer user to be using the local Email client. Emails sent by this mechanism (and therefore personal user information) may be retained in the Email client's Sent Mail folder.

Feature Location Email can be accessed using either the File > Email menu entry, or by clicking the Email icon in the toolbar.





Method for Reducing Exposure

Hide the “Email…” menu entry in the File menu and the Email icon from the Toolbar. This can be done using a folder-level JavaScript with the following line items:

```
app.hideMenuItem("AcroSendMail:SendMail");
app.hideToolbarButton("AcroSendMail:SendMail");
```

Comments

See “Adding JavaScript Scripts” on page 2.

Send for Review

Feature

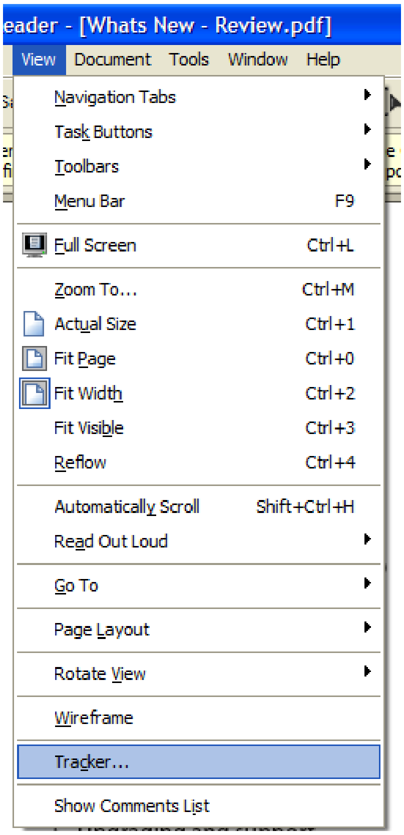
If a user opens a PDF enabled for review (enabled via Reader Extension Server or Acrobat’s Send for Review capability), Reader will allow the user to save comments and send comments. Reader can also retain the status of this document in the Review Tracker.

Possible Information Exposure

If the PDF enabled for review is saved locally, Tracker will retain information about that PDF. If that PDF is returned by Email or is not saved, Tracker will not retain that information. If another user then opens up an enabled PDF and also opens Tracker, this new user will see information on the previous review workflow.

Feature Location

When an enabled PDF is opened in Reader, the Review Tracker becomes available under View > Tracker (menu selection shown below):



Method for Reducing Exposure

Hide "Tracker..." in the View menu using the following folder-level JavaScript:

```
app.hideMenuItem("Annots:ReviewTracker");
```

Comments

See "Adding JavaScript Scripts" on page 2.

Spell Checking Dictionary

Feature

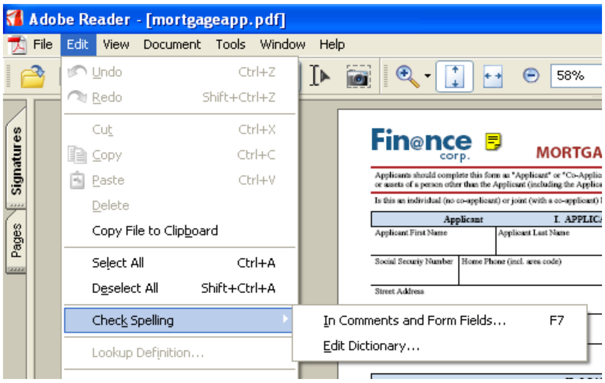
When spell checking form fields or annotations in an enabled PDF, a user can add frequently-used words to the dictionary to improve performance.

Possible Information Exposure

Users can customize the spelling dictionary to improve performance. If the added entry is sensitive text, such as a person's or company's name, other users would be able to see it by selecting Edit > Check Spelling > Edit Dictionary.

Feature Location

Spell checking can be started by clicking Edit > Check Spelling.



The user can then either start the spelling check and optionally add corrected words to the dictionary, or add words directly to the dictionary using: Edit > Check Spelling > Edit Dictionary.

Method for Reducing Exposure

Hide the Spelling Check menu item using the following folder-level JavaScript script:

```
app.hideMenuItem("Spelling:Spelling");
```

Comments

Hiding the menu item will hide the Check Spelling menu item. There is a keyboard shortcut to check spelling for form fields and annotations (F7), but the resulting dialog window does not give the user the option to add to or edit the spelling dictionary.

See “Adding JavaScript Scripts” on page 2.

Digital Signatures

Feature

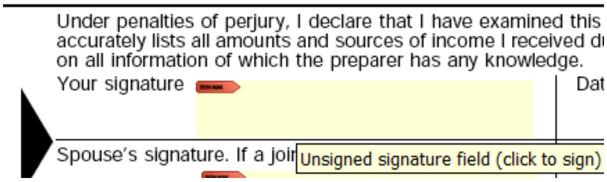
If a user opens a PDF enabled for digital signatures by Acrobat Professional or LiveCycle server products, Reader will allow the user to create or access a digital signature, and then sign and save the PDF.

Possible Information Exposure

During the signing workflow, the user is prompted to create a self-sign digital ID, browse for an existing digital ID, or purchase a digital ID. One result is that the digital ID can be saved on the local machine, where it can be viewed and accessed by other users.

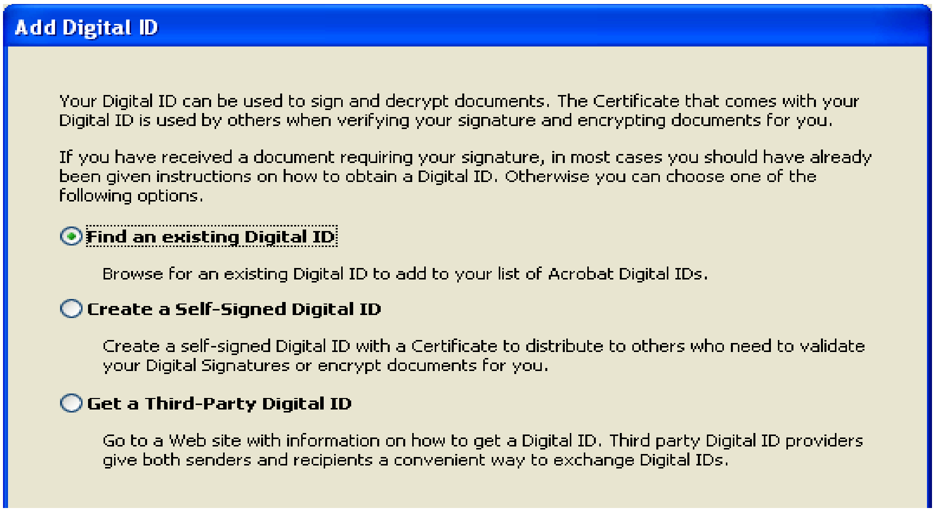
Feature Location

When an enabled PDF is opened in Reader and the user clicks on a signature field such as shown below:



Under penalties of perjury, I declare that I have examined this
accurately lists all amounts and sources of income I received d
on all information of which the preparer has any knowledge.
Your signature
Dat
Spouse's signature. If a joir
Unsigned signature field (click to sign)

The user is then prompted to create, browse to, or purchase a digital ID as shown in the Add Digital ID window shown below:



Add Digital ID

Your Digital ID can be used to sign and decrypt documents. The Certificate that comes with your Digital ID is used by others when verifying your signature and encrypting documents for you.

If you have received a document requiring your signature, in most cases you should have already been given instructions on how to obtain a Digital ID. Otherwise you can choose one of the following options.

● Find an existing Digital ID

Browse for an existing Digital ID to add to your list of Acrobat Digital IDs.

○ Create a Self-Signed Digital ID

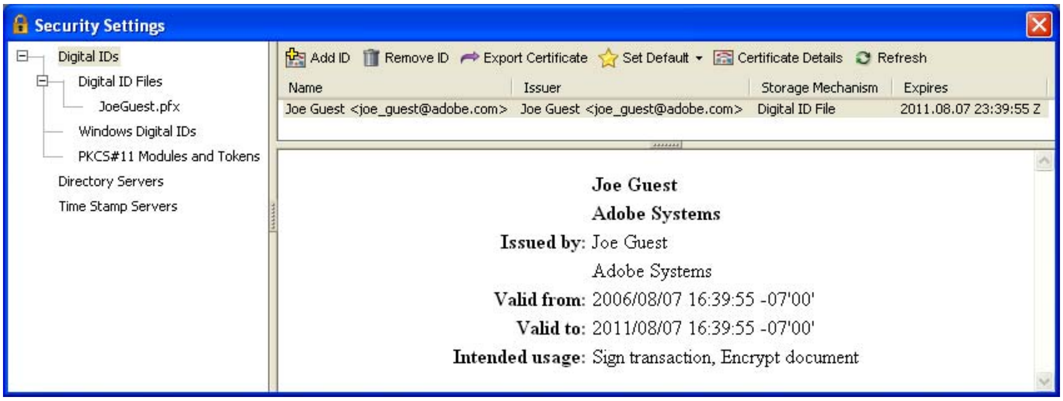
Create a self-signed Digital ID with a Certificate to distribute to others who need to validate your Digital Signatures or encrypt documents for you.

○ Get a Third-Party Digital ID

Go to a Web site with information on how to get a Digital ID. Third party Digital ID providers give both senders and recipients a convenient way to exchange Digital IDs.

If a user *browses to a digital ID* (on the local drive or on an external drive, like a USB token), that digital ID is in most cases not copied into Reader. Reader references that digital ID for signing, but then deletes that reference when the digital ID is removed from the local or external drive.

If a user *creates a digital ID*, it is added to Reader's store of digital IDs. It then becomes viewable by other users under Document > Security Settings > Digital IDs. However, other users cannot apply it without knowing the Password.



Name	Issuer	Storage Mechanism	Expires
Joe Guest <joe_guest@adobe.com>	Joe Guest <joe_guest@adobe.com>	Digital ID File	2011.08.07 23:39:55 Z

Joe Guest
Adobe Systems
Issued by: Joe Guest
Adobe Systems
Valid from: 2006/08/07 16:39:55 -07'00'
Valid to: 2011/08/07 16:39:55 -07'00'
Intended usage: Sign transaction, Encrypt document

Method for Reducing Exposure

The Windows registry can be set to prevent users from creating a self-signed digital ID. To set that registry key, under:

```
HKEY_USERS\<numeric key[a]>\Software\Adobe\Acrobat
Reader\7.0\Security\cPubSec
```

create a `dword: bSelfSignCertGen` and set the value to false.

Optional:

The digital ID menu items can be hidden to prevent the user from browsing to Security Settings. Use the following folder-level JavaScript:

```
app.hideMenuItem("ppklite:UserSettings");
app.hideMenuItem("DIGSIG:DigitalSignatures");
```

Comments

Users cannot edit the registry. See “Editing the Registry” on page 3.

If the user is logged in as User, Acrobat’s JavaScripts folder cannot be changed, and there is no keyboard shortcut for this feature. See “Adding JavaScript Scripts” on page 2.

[a] This key’s name is an alphanumeric of the form: S-1-5-21-762979615-2031575299-929701000-1006. It is found under HKEY_USERS, and is not the one with the “_Classes” suffix, and it will have a “+” before the key name.

Trusted Identities

Feature

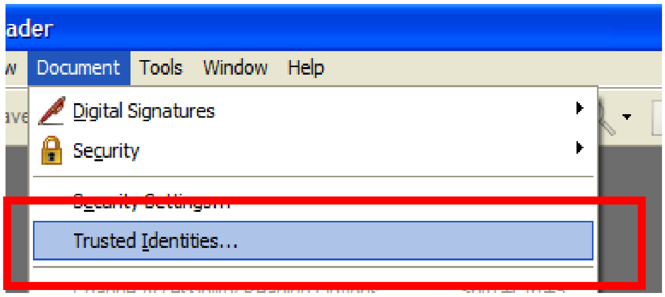
The user has the ability to add certificates from other users into a Trusted Identities area in order to more quickly validate signed PDF files.

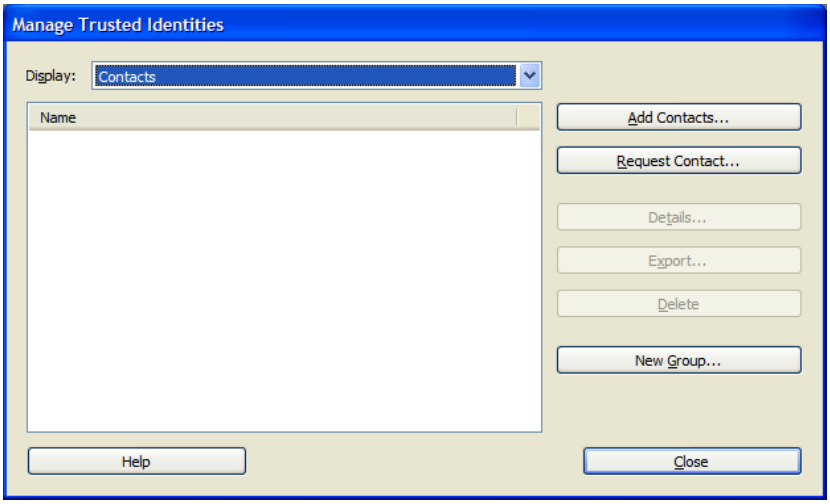
Possible Information Exposure

Adding someone to the Trusted Identities list would only expose information contained in their public key, which is not confidential information. It only reveals that the user might have expected to exchange signed documents with those persons, not whether any document was signed or exchanged.

Feature Location

A certificate can be added to Trusted Identities by accessing it under Document > Trusted Identities:





Display: Contacts

Method for Reducing Exposure

The menu item for Trusted Identities can be hidden using a folder-level JavaScript script:

```
app.hideMenuItem("PUBSEC:AddressBook");
```

Comments There is no keyboard shortcut for this feature, so users cannot access it using the keyboard. See “Adding JavaScript Scripts” on page 2.

Policy Server Access

Feature If a user opens a PDF file encrypted using Adobe LiveCycle Policy Server, that user will be prompted to provide a user name and password in order to open that file. Reader can also cache that password so that re-opening that same file will not require the user to re-enter the password.

Possible Information Exposure If the user caches their password, a later user can re-open that PDF file without being prompted to enter a password.

Method for Reducing Exposure The Windows registry can be edited so a user cannot cache their password. To set that registry key, under

```
HKEY_USERS\<xxxxx>\Software\Adobe\Acrobat
Reader\7.0\Security\cPPKLite
```

create a `dword: bAllowPasswordSavingDefault`

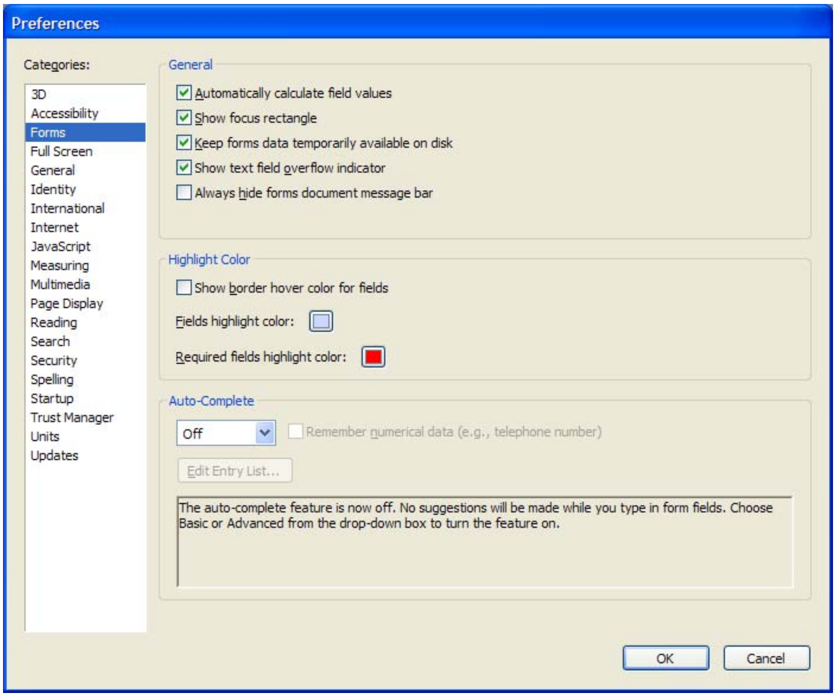
and set the value to false.

Forms

Feature When a PDF form is filled in, there are various options to retain form data, and the Auto-complete feature may be turned on.

Possible Information Exposure On a public machine, it is not appropriate to retain form data after the user’s session has ended, so Auto-complete should not be enabled.

Feature Location In Edit > Preferences > Forms, the value “Keep forms data temporarily available on disk” is ON by default. In that same location, Auto-complete is OFF by default.



General

☑ Automatically calculate field values

☑ Show focus rectangle

☑ Keep forms data temporarily available on disk

☑ Show text field overflow indicator

☐ Always hide forms document message bar

Highlight Color

☐ Show border hover color for fields

Fields highlight color: 🟦

Required fields highlight color: 🟥

Auto-Complete

Off

☐ Remember numerical data (e.g., telephone number)

The auto-complete feature is now off. No suggestions will be made while you type in form fields. Choose Basic or Advanced from the drop-down box to turn the feature on.

Method for Reducing Exposure

Turn off forms data caching. Turn off Reader’s caching of forms data using page-open or folder-level JavaScript placed in Reader’s JavaScripts folder:

```
this.nocache = true;
```

The advantage of using this script is that it does not affect the checkbox item: “Keep forms data temporarily available on disk” (located under File > Preferences > General > Forms).

Turn off preference for keeping forms data: turn off Auto-Complete. Make sure that Auto-Complete is off using the following page-open or folder-level JavaScript:

```
this.noautocomplete = true;
```

When set to true, no suggestions are made as the user enters data into the field. If this property is set to false, Reader respects the user preference set under File > Preferences > General > Forms.

NOTE: For Adobe LiveCycle Designer forms, use the following JavaScript code:

```
var oDoc = event.target;
oDoc.nocache = true;
```

Optiona l:

Edit registry to lock Auto-Complete. Set the Auto-Complete lockdown key in the registry to disable Auto-Complete; to prevent users from turning it back on, and to disable the prompt to turn on Auto-complete when the user begins to fill out the form. At the key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\
Adobe Reader\7.0\FeatureLockdown
```

create a dword "`bAutoFill`" and set its value to 0.

Hide Preferences menu item. Hide Preferences from Edit menu using folder-level JavaScript:

```
app.hideMenuItem("GeneralPrefs");
```

NOTE: Caching will not occur if the document is loaded from an HTTPS site.

Comments

When the Preferences menu item is hidden, users can access it using the keyboard shortcut Ctrl-k.

See "Adding JavaScript Scripts" on page 2.

Auto-save File Changes

Feature

User has the option to "Auto-save file changes to temp file". That value can be set between 1 and 99 minutes. The default is 5 minutes.

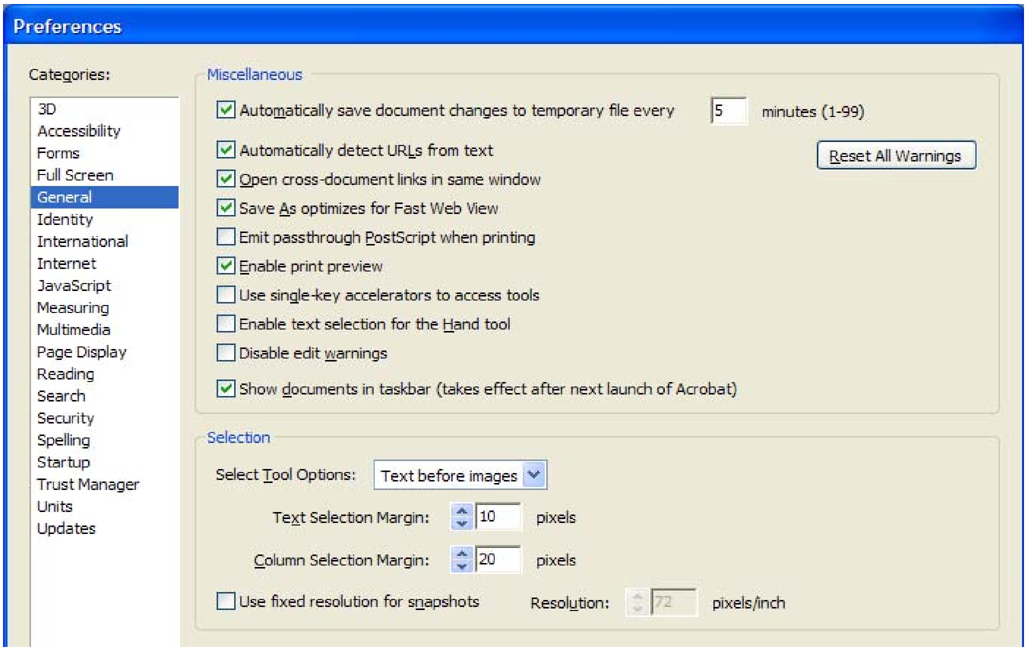
Possible Information Exposure

Changes made to a PDF document beyond the current state of the file are saved to a temp file.

The Auto-save feature is only a problem if the document is a Reader enabled PDF; otherwise data cannot be changed or saved. If the document is enabled, form data could be stored in a temp file. With Reader 7.0, temp files are not removed after a system crash, so they can persist.

Feature Location

Under Edit > Preferences > General:



Miscellaneous

☑ Automatically save document changes to temporary file every 5 minutes (1-99)

☑ Automatically detect URLs from text

☑ Open cross-document links in same window

☑ Save As optimizes for Fast Web View

☐ Emit passthrough PostScript when printing

☑ Enable print preview

☐ Use single-key accelerators to access tools

☐ Enable text selection for the Hand tool

☐ Disable edit warnings

☑ Show documents in taskbar (takes effect after next launch of Acrobat)

Selection

Select Tool Options: Text before images

Text Selection Margin: 10 pixels

Column Selection Margin: 20 pixels

☐ Use fixed resolution for snapshots Resolution: 72 pixels/inch

Method for Reducing Exposure

In the User account, Administrator can uncheck the box to automatically save document changes to a temporary file.

Search: Cache Index Information

Feature

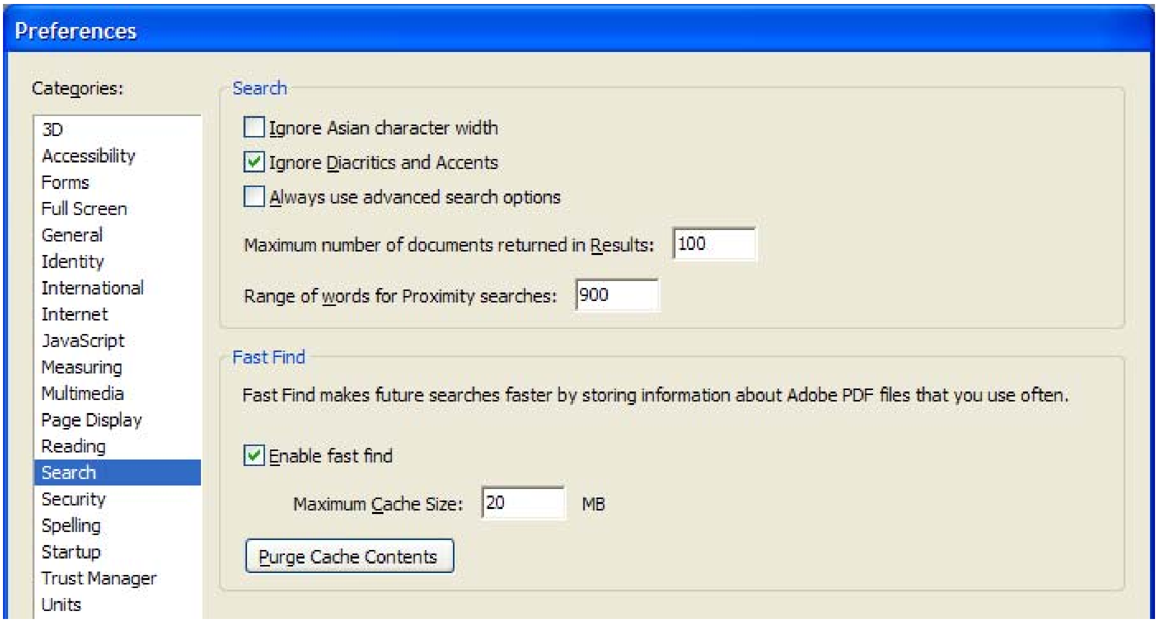
The User has the option to cache file search index information to a file to speed up subsequent searches. This option is On by default. The cache file would contain the words searched for and the search context information, as well as pointers to the files involved. The resulting cache file will persist on the system and be available to other users. However, the file is written using a proprietary format, so only reverse-engineering would reveal the contents.

Possible Information Exposure

On a public computer, it is not appropriate to cache the search file contents.

Feature Location

Under Edit > Preferences > Search, you will see the preferences dialog window as follows:



Search

□ Ignore Asian character width

☑ Ignore Diacritics and Accents

□ Always use advanced search options

Maximum number of documents returned in Results: 100

Range of words for Proximity searches: 900

Fast Find

Fast Find makes future searches faster by storing information about Adobe PDF files that you use often.

☑ Enable fast find

Maximum Cache Size: 20 MB

Method for Reducing Exposure

Turn Off Fast Find in Reader's Preferences window shown above. The Preferences item in the menu can be hidden, but a user can access it using the keyboard shortcut (Ctrl-k).

Recently Opened Files

Feature

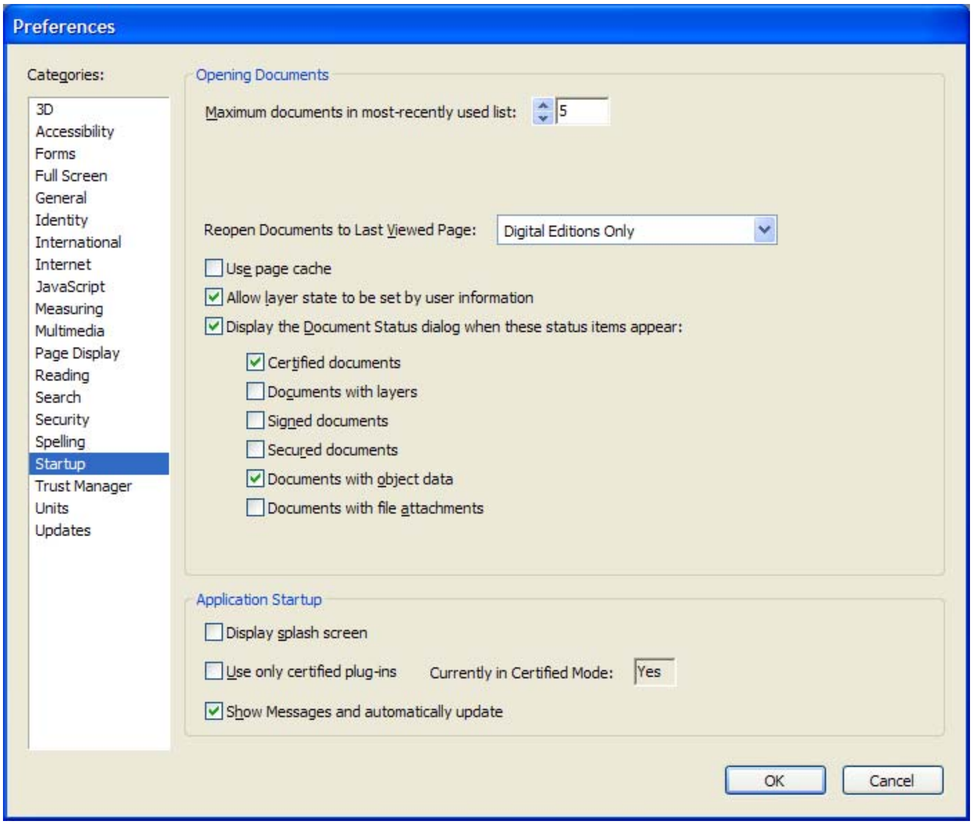
Reader will retain a list of the most recently opened files. The file names are used to populate a pop-up menu when the user selects File > Open. The value can be set between 1 and 10 files. The default is 5.

Possible Information Exposure

This list of recently opened files is viewable by other users.

Feature Location

Under Edit > Preferences > Startup



Preferences

Opening Documents

Maximum documents in most-recently used list: 5

Reopen Documents to Last Viewed Page: Digital Editions Only

□ Use page cache
☑ Allow layer state to be set by user information
☑ Display the Document Status dialog when these status items appear:

- ☑ Certified documents
- □ Documents with layers
- □ Signed documents
- □ Secured documents
- ☑ Documents with object data
- □ Documents with file attachments

Application Startup

□ Display splash screen
□ Use only certified plug-ins   Currently in Certified Mode: Yes
☑ Show Messages and automatically update

Method for Reducing Exposure

System administrator can set the value to 1 (the number of recently opened files to remember).

URL Trust Manager

Feature

User can specify preference for whether Reader can connect to web sites to send or get data.

Possible Information Exposure

When the user encounters a PDF document that attempts to send or receive data from an external Web site, the default is for Reader to prompt the user if they want to allow or block that action. There is a check box asking if they wish to remember their choice to allow or block that site. If they do check the box, URLs will be saved by the URL Trust Manager, and could be seen by other users.

Feature Location

User can set preferences by selecting Preferences > Trust Manager, and then in the Resource Access pane, clicking Change Site Settings.

Method for Reducing Exposure

Lock the URL Trust Manager by locating the following key in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Adobe\Adobe
Acrobat\7.0\FeatureLockDown\cDefaultLaunchURLPerms
```

create the dword: `iUnknownURLPerms` and set it's value to true.

Comments

With that setting of the registry, the user will continue to be prompted as to whether or not they wish to allow or block the site, but the check box will be disabled. As a result, Reader will not save the URL of sites visited.

Collected Scripts

The scripts recommended in this document are collected below to make it easier for you to cut and paste the ones you need.

```
// Hide the Preferences menu item
app.hideMenuItem("GeneralPrefs");
// Hide the Email and toolbar items
app.hideMenuItem("AcroSendMail:SendMail");
app.hideToolbarButton("AcroSendMail:SendMail");

// Hide the Review Tracker
app.hideMenuItem("Annots:ReviewTracker");

// Hide the Spelling Check menu item
app.hideMenuItem("Spelling:Spelling");

// Hide the digital ID menu item
app.hideMenuItem("ppklite:UserSettings");
app.hideMenuItem("DIGSIG:DigitalSignatures");
 // Hide the Trusted Identities menu item
app.hideMenuItem("PUBSEC:AddressBook");

// Turn off Auto-Complete
this.noautocomplete = true;

// Turn off Acrobat's forms caching
this.nocache = true;
```

References

JavaScript for Acrobat API Reference

Developing Acrobat Applications with JavaScript

Available at:

http://www.adobe.com/devnet/acrobat/javascript.html

InstallShield Tuner 7.0 for Adobe Acrobat

Available at the Adobe Acrobat Enterprise Deployment support page:

http://www.adobe.com/devnet/acrobat/enterprise_deployment.html

Copyright 2006 Adobe Systems, Incorporated. All rights reserved.

Adobe Systems Incorporated
345 Park Avenue, San Jose, CA 95110-2704 USA
http://www.adobe.com

Adobe, the Adobe logo, Acrobat, Adobe Reader, Adobe LiveCycle, and Adobe LiveCycle Policy Server, and are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks are the property of their respective owners.

8 December 2006