Enhanced Security Quick key

What?

Enhanced security was introduced with 9.0 and 8.1.7 (enabled by default in 9.3/8.2). It provides a set of restrictions that blocks potentially dangerous actions and hardens the application to prevent cross domain access (requested content must adhere to a “same-origin” policy), silent printing, high privilege JavaScript execution, script and data injection, and stream access to Xobjects.

The product’s trust model provides a mechanism, called “Privileged Locations”, that enables assigning trust to files, folders, and hosts that should not be subject to those restrictions.

User Interface Configuration[1]

To configure enhanced security (Win and Mac only):

1: Navigate to the preferences panel.

2: Choose **Security (Enhanced)**.

3: Check/uncheck **Enable Enhanced Security**.

4: Check **Create log file** to enable cross domain logging.

To bypass enhanced security restrictions for trusted content:

1: Choose whether to trust sites you already trust in IE.

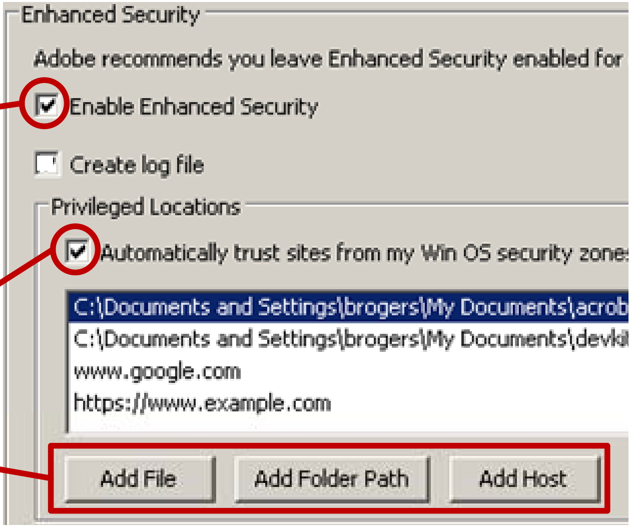
Introduced with 9.3/8.2 for Mac and UNIX

2: Choose whether to trust certified documents with a valid signature.

Introduced with 11.0

3: Choose **Add File**, **Add Folder Path**, or **Add Host**.

4: Specify or select a location that contains trusted content.



Enhanced Security

Adobe recommends you leave Enhanced Security enabled for

☑ Enable Enhanced Security

☐ Create log file

Privileged Locations

☑ Automatically trust sites from my Win OS security zone

C:\Documents and Settings\brogers\My Documents\acrob
C:\Documents and Settings\brogers\My Documents\devki
www.google.com
https://www.example.com

Registry Configuration[4]

Registry-level preferences provide Admins with granular control over the feature. High level rules:

- ✓ Windows, Macintosh, and UNIX platforms use similarly named keys.
- ✓ When configuring paths, use your product (Adobe Acrobat or Acrobat Reader) and version (e.g. 11.0).
- ✓ For 8.x, **only** one key (bEnhancedSecurityStandalone) controls behavior for both standalone and browser modes.
- ✓ Preferences are boolean. True (1) enables the feature. False (0) disables the feature.

Windows

To disable Enhanced Security: (Example uses Acrobat and any 9.x version)

Path for keys tied to user the interface: [HKEY_CURRENT_USER\Software\Adobe\Adobe Acrobat\9.0\TrustManager]

```
   "bEnhancedSecurityInBrowser"=dword:00000000
   "bEnhancedSecurityStandalone"=dword:00000000
```

To disable and lock Enhanced Security: (Example uses Reader and any supported 11.x version)

Path for lockable keys: [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\Acrobat Reader\11.0\FeatureLockDown]

```
   "bEnhancedSecurityStandalone"=dword:00000000
```

To disable and lock privileged locations (Gives admin control over what is trusted when ES is enabled):

```
   "bDisableTrustedFolders"=dword:00000001
   "bDisableTrustedSites"=dword:00000001
```

Macintosh

To disable Enhanced Security:

Mactel root: User\Library\Preferences\com.adobe.Acrobat.Pro_x86_9.0.plist

PowerPC root: User\Library\Preferences\com.adobe.PPC.plist

TrustManager > EnhancedSecurityInBrowser: Boolean: NO.

TrustManager > EnhancedSecurityStandalone: Boolean NO.

UNIX

Root path: ~/.adobe/Acrobat/9.0/Preferences/reader_prefs

Enhanced security disabled:

```
/TrustManager   [/c << /EnhancedSecurityInBrowser [/b false]  /EnhancedSecurityStandalone [/b false]  >>]
```

Server Config.[2]

Cross domain access can be managed by a server’s cross domain policy.

- ✓ The file must be named crossdomain.xml and reside at the server root. http://example.com/crossdomain.xml should display the file.
- ✓ The MIME type and file syntax must conform to the specification.
- ✓ Enable logging to AcrobatCrossDomain.log via the UI (9.3/8.2) or the registry (9.x and 8.1.7) (AVPrivate/bCrossDomainLogging=true).

References

Application Security Guide

Preference Reference for Acrobat & Reader

Cross Domain Policy File Specification