Enhanced Security Troubleshooting Guide and FAQ

CONTENTS

1 Enhanced security: why and what?
2 Best practices
2 Application configuration and troubleshooting
7 Server configuration and troubleshooting
8 Bypassing enhanced security restrictions
10 Workflow fixes with enhanced security enabled
12 Additional resources

This document is intended for users who encounter problems with documents and workflows when enhanced security is enabled for Acrobat or Adobe Reader. As of the 9.3 and 8.2 updates, enhanced security will be automatically enabled by Adobe. Because enhanced security restricts certain features and document behavior, some users may encounter broken workflows or unfamiliar dialogs. These FAQs attempt to address any questions which may arise.

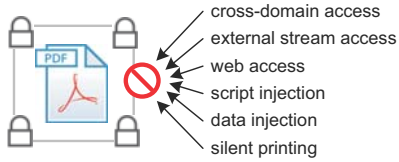
Tip: For a companion document, see Enhanced Security and Trusted Locations.

Enhanced security: why and what?

Enhanced security consists of two components: a set of default restrictions and a method to define trusted locations that should not be subject to those restrictions. In other words, you can either block dangerous actions altogether or else selectively permit them for locations and files you trust.

With enhanced security enabled, your application "hardens" itself against risky actions by doing the following for any document not specifically trusted:

- Prevents cross domain access. It forces requests for new content to adhere to a "same-origin" policy; that is, access to web pages and other resources originating from a domain other than your calling document is prohibited.
- Prohibits script and data injection via an FDF, XFDF, and XDP NOT returned as the result of a post from the PDF.
- Blocks stream access to XObjects such as external images.
- Stops silent printing to a file or hardware printer.
- Prevents execution of high privilege JavaScript.

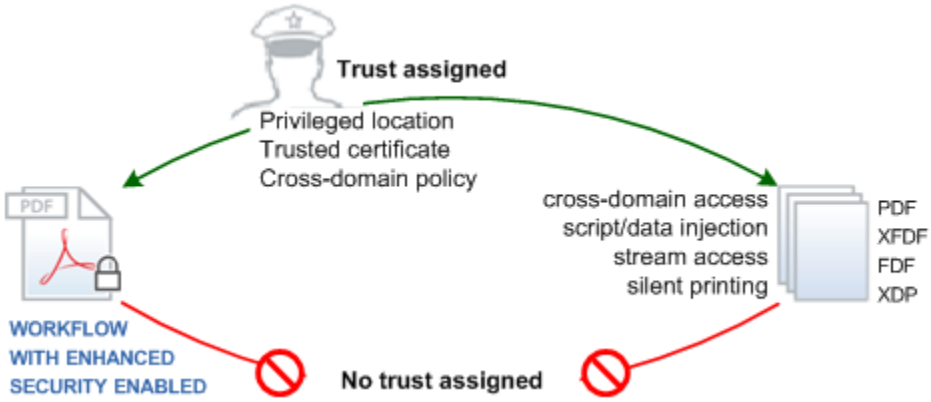


New security model

These protections are targeted at protecting users against popular web attacks such as cross site scripting and cross site request forgeries. When enabled, enhanced security may affect legacy and new PDF workflows. It is specifically designed to let you decide what content to trust and help you selectively bypass those restrictions for trusted files, folders, and hosts. These trusted domains--called privileged locations--are exempt from enhanced security rules. There are several other methods for establishing

trust, and just as you tune your browser, so should you tune your application so that it operates at a risk level appropriate for your environment.

Figure 1 Enhanced security: effect on worklfows



Enhanced security configuration can occur via the user interface (UI) by end users. However, in enterprise settings, administrators will likely want to tune the preferences at the registry level. Doing so not only provides a more fine grained control, it also provides the means lock those preferences so that they cannot be changed via the UI. When properly configured for your workflows, malicious attacks such as cross site scripting are prevented, and a rich user experience is provided in the context of a safe and trusted environment.

This feature interacts with other features that also assign trust. When content is trusted as a result of a cross domain policy file for example, that content is not subject to enhanced security restrictions. It is important to understand the various ways that trust can be assigned prior to configuring applications and setting up workflows. Workflows should be designed for compatibility with enhanced security enabled, so keep in mind that the following features interact with enhanced security:

- **Internet access permissions**: While enhanced security prevents access to different origin locations that try to return data, scripts, or content to the calling PDF, internetaccess ingeneal can be set on a per site basis via the Trust Manager. Trust Manager settings may or may not override enhanced security setting depending on your application version and particular workflow.
- **Import and export of FDF, XFDF (form), and XDP data**: Data file behavior is fundamentally altered when this feature is on.
- **Certified document workflows**: Access to a certified document may or may not be allowed depending on whether:
  - The signing certificate's fingerprint is in a cross domain policy file, or
  - The signing certificate is trusted or chain's up to a trust anchor that is trusted for privileged networked operations.

Best practices

To maintain workflow security, the following is recommended:

- Enhanced security should be enabled on all clients.

- All workflow components such as forms, form data, remotes host, and so on should be pre assigned trust.
- Administrators should manage trust via a server-based cross domain policy file if possible.

Application configuration and troubleshooting

Is enhanced security supported on all versions of Acrobat and Adobe Reader?

No. Enhanced security is only available for 9.x and 8.1.7 Acrobat and Adobe Reader on Windows, Macintosh, and UNIX (and later). It is not supported in earlier product versions.

Is enhanced security automatically enabled, or do I have to do it manually?

This feature is automatically enabled for Acrobat and Adobe Reader 9.3 and 8.2. All other users should manually enable the feature.

How do I enable or disable enhanced security via the user interface?

1. Navigate to the preferences panel. The method to do so varies by product and platform.
2. Choose **Security (Enhanced)**.
3. Check or uncheck the **Enable Enhanced Security** checkbox (Figure 10).

> **Caution:** Turning off enhanced security enables a number of risky behaviors, including unrestricted cross domain access. For more information, refer to Enhanced Security and Trusted Locations.

How do I enable or disable enhanced security via the registry or plist?

As described in Enhanced Security and Trusted Locations, all aspects of enhanced security be configured at the registry level, including privileged locations. The following two keys control enhanced security:

- **bEnhancedSecurityInBrowser**: Controls enhanced security for the application in the browser.
- **bEnhancedSecurityStandalone**: Controls enhanced security for the standalone application.

These keys may reside in two locations on Windows:

- HKCU\Software\Adobe\(product name)\(version)\TrustManager: A user setting that is subject to modification via the user interface.
- HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Adobe\(product name)\(version)\FeatureLockDown\: An administrator-only setting that locks the user interface so that users can't change the setting.

Why does my document do things I think it shouldn't do, such as access certain web sites?

Many of the security tools interact with each other. In some cases, the most permissive setting takes place; in others, the least permissive. For example, what URLs you can access can be affected by settings in enhanced security, trust manager, and the trusted identity manager (for certificates). You should familiarize yourself with all the tools and configure the application to behave as needed.

Why does my document not do things I think it should do, such as access certain web sites?

See above. See also Bypassing enhanced security restrictions.

Why does form data disappear when I choose to trust a document or host once or always?

See Workflow fixes with enhanced security enabled.

Why doesn't my certified document override enhanced security restrictions?

A certification can only exempt a document from enhanced security restrictions if the signing certificate is trusted for privileged network operations. Open the Trusted Identies Manager and set its trust level.

Why won't my flash content run for a document that's in a privileged location?

The Flash security model always requires the use of a server based cross domain policy when the player tries to access content and data that originates from a different origin (domain).

How come rich media annotations (RMA) (embedded flash) won't run?

Cross domain checks are done for RMA's, so trust must be assigned via a cross domain policy file, privileged locations, or certification.

Why is my FDF, XFDF, or XDP file workflow broken?

Enhanced security changes the way these files are handled because they have the capability to open other files and inject scripts and data (Figure 1). To address the issue, allow access to the file by one of the methods described in Client controls. For details about file behavior with respect to enhanced security, see Enhanced Security and Trusted Locations.

Why do I see a warning dialog that says I can't access scripts, data, or other documents?

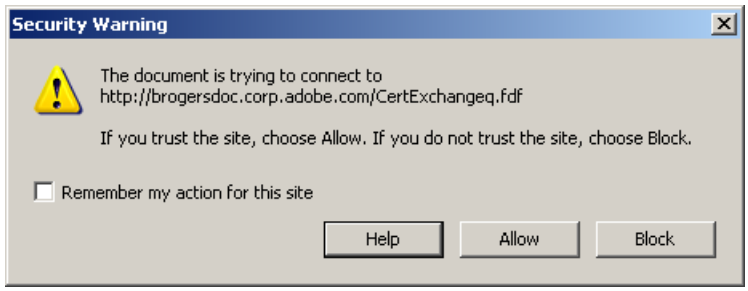
Enhanced security restricts several kinds of potentially risky behaviors. When a PDF file tries to do something that enhanced security blocks, a dialog or Yellow Message Bar appears. These actions include script injection and execution (access to JavaScript), cross domain access (whether documents, data, FDFs, and external streams), and silent printing. To allow the action indicated by the dialog, trust the content at the client or server level as described in Bypassing enhanced security restrictions.

The warning dialogs are shown here:

- Warning dialogs: basic URL connection (all versions)
- Warning dialogs: for 9.2 and 8.1.7 patches and later
- Warning dialogs: for 9.2 and 8.17 patches and earlier

Warning dialogs: basic URL connection (all versions)

Figure 2 Security warning: Basic link with no return data



Warning dialogs: for 9.2 and 8.1.7 patches and later

The **Options** button only appears if the administrator has not disabled the end uses ability to set trust. Selecting "Always" adds the document to the privileged locations list.

Figure 3 Yellow Message Bar: With no user override

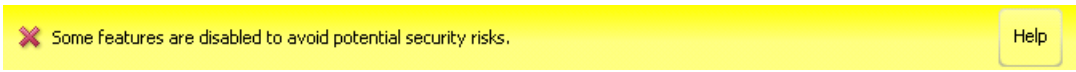


Figure 4 Yellow Message Bar: with user override

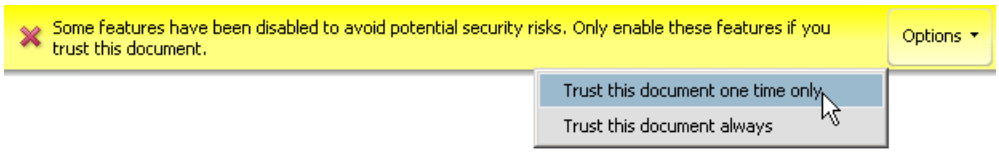


Figure 5 Yellow Message Bar: JS with no user override

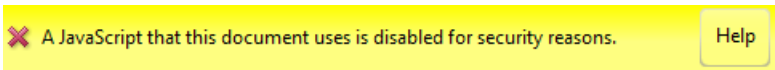
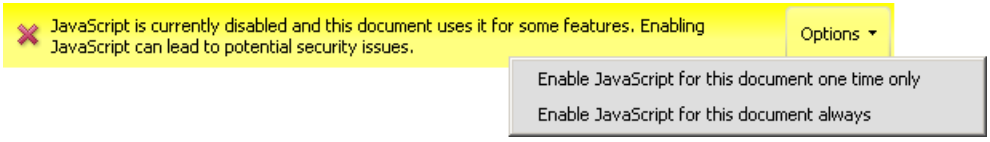


Figure 6 Yellow Message Bar: JS with user override



Warning dialogs: for 9.2 and 8.17 patches and earlier

Figure 7 Enhanced Security Block dialog: JavaScript access

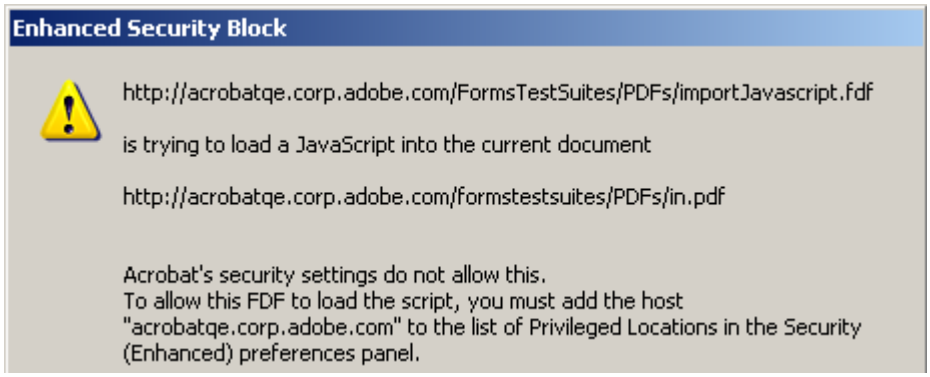


Figure 8 Security Warning dialog: Cross domain access

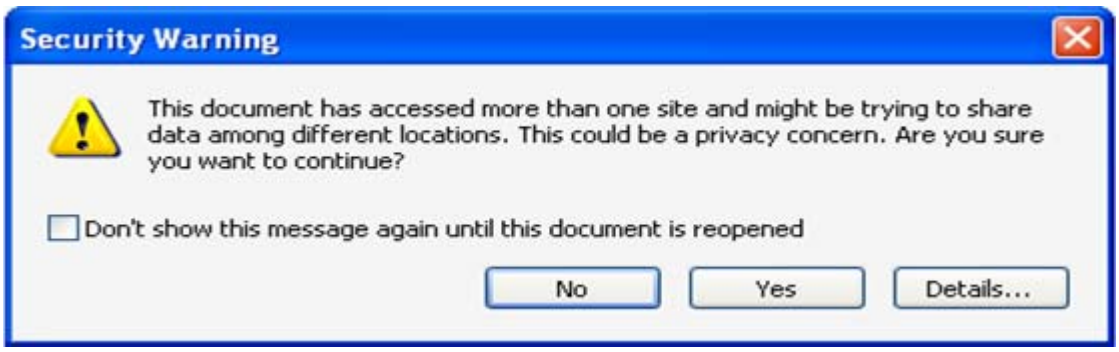
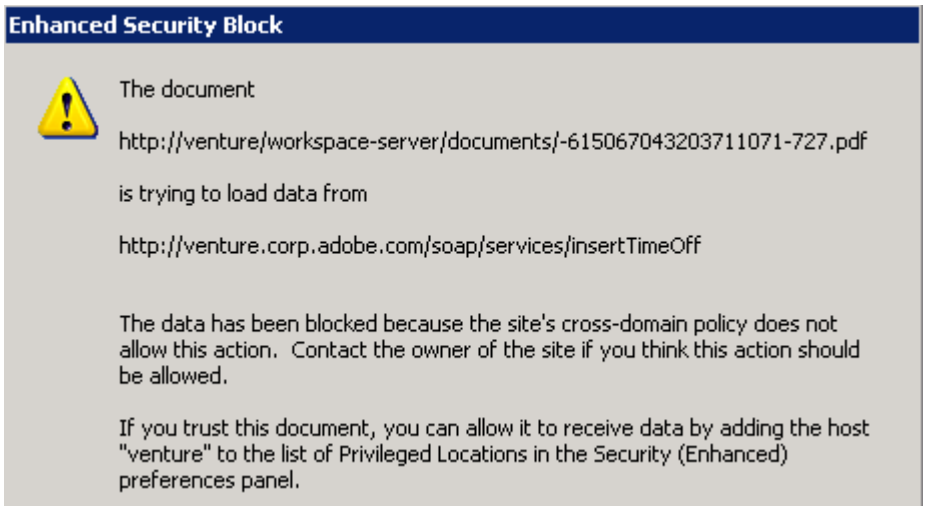


Figure 9 Enhanced Security Block dialog: Data access



Administrator-only client FAQs

How do I configure clients before deployment?

The application installer can be tuned prior to distribution with the Adobe Customization Wizard 9.

How do I configure clients after they are deployed?

You can fine tune existing installations to provide restrictions and enable features for trusted documents. Post deployment methods of configuration include the following:

- Manual configuration on a case by case basis.
- Pushing registry/plist changes out using any applicable scripting mechanism.
- Exporting security settings from a "template" application and then importing those settings on machines as needed via the Import Security Settings feature. For details, see the Digital Signatures and Rights Management in Acrobat and Adobe Reader.

I need to prevent users from changing settings. How?

Many security settings are lockable so that the end user cannot change them through the user interface. Because the lock is found in the HKLM section of the registry under FeatureLockdown, only a user with administrator rights can modify the setting. You can lock down features pre-deployment by tuning the installer with the Customization Wizard, or you can lock them post-deployment as described above.

Note: There is a current bug in which the enhanced security user interface does not appear to be locked (disabled) After locking. However, locking the feature does work.

How can I fine tune security at a more granular level than is available via the UI?

An administrator can tune the client at the registry or plist level. For details, refer to the appropriate document listed in Additional resources.

Server configuration and troubleshooting

How do I control cross domain access at the server level?

Controlling access to cross-domain content involves turning on enhanced security and then trusting content for specific domains either at the client or server level. Server configuration requires that an administrator construct a cross domain policy file that conforms to Adobe's specification and then locate that file on the server. For details, see the following:

- Cross-domain Access and Configuration: A technical guide client and policy file configuration.
- Cross-domain Policy File Specification: A specification for Acrobat/Reader X-domain policy files.

How do I enable cross domain logging?

Logging is useful for troubleshooting server-based policy files even though logging is configured and occurs on the client. For example, logs can tell you if the MIME type or syntax of the cross domain file is incorrect. For details, see Cross-domain Access and Configuration.

What is the proper MIME type for a cross domain policy file?

The file MIME type should be set to

- 9.2/8.17: `text/x-cross-domain-policy`
- 9.3/8.2: Any type supported by the specification.

For details, see Cross-domain Access and Configuration.

Does the cross domain policy file support aliases and "friendly" names?

Yes. However, that support must be configured. Just as you specify accessible fully qualified domain names (FQDN), simply provide the aliases and friendly names you wish to support. For example:

```
<allow-access-from domain="<your FQDN>" />
<allow-access-from domain="http://humanresources" />
<allow-access-from domain="hr" />
<allow-access-from domain="humanresources" />
<allow-access-from domain="<any friendly name/alias your server can resolve>" />
```

Where do I locate the cross domain policy file?

At the root of the server. However, what constitutes the root may vary with the application server you are using. For example, installations may look like this:

- **Jboss**: ...\jboss\server\lc_turnkey\deploy\jboss-web.deployer\ROOT.war\crossdomain.xml
- **SAP Netweaver**: C:\usr\sap\<Server ID>\J00(JC00 for Netweaver 7.0)\j2ee\cluster\apps\sap.com\com.sap.eng\crossdomain.xml

Note: For additional examples, see Cross-domain Access and Configuration.

Bypassing enhanced security restrictions

Because enhanced security limits functionality and restricts certain operations, you can use one of several mechanisms to override those restrictions for content you specifically trust, including:

- Client controls:
  - Specifying privileged locations
  - Specify trusted URLs via Trust Manager
  - Trusting certificates for privileged network operations
- Server controls:
  - Managing cross domain access at the server
  - Enabling cross domain access for specific PDFs

Client controls

Specifying privileged locations

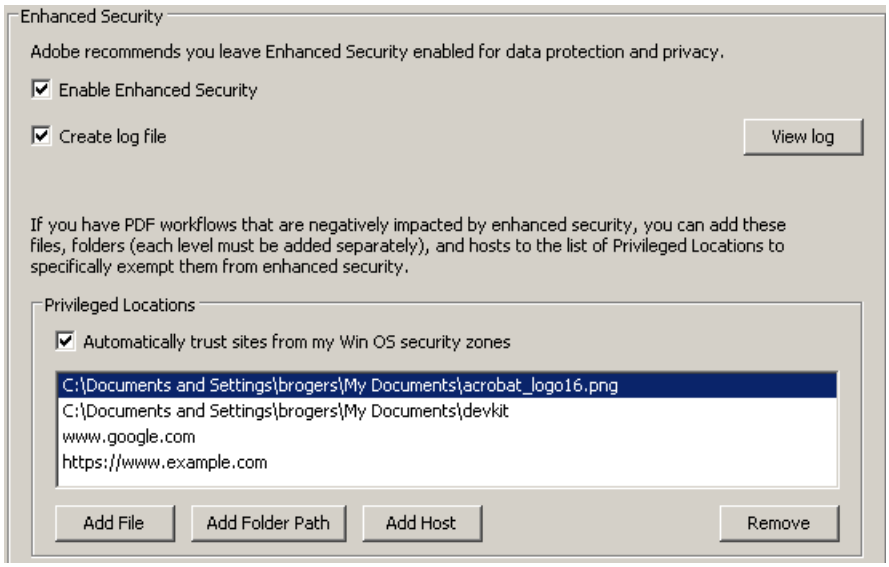
Enhanced security provides a method for specifying locations for trusted content. Privileged locations can be a single file, a directory, or a host. The application maintains two privileged location lists: an administrator list (in HKLM) and a user list (in HKCU). The user list is for the current user only and can be edited via the user interface. The default installation does not specify any privileged locations.

The administrator list is created manually or by tuning the installer with the Acrobat Customization Wizard before deployment. This method of trusting content is beneficial for administrators that control clients in closed workflows, that don't own a web service and so can't manage a cross domain policy, who need to grant rights such as silent printing, and who trust the location. For more details, see Enhanced Security and Trusted Locations.

To specify a privileged location through the user interface:

1. Navigate to the enhanced security panel.
2. Set a privileged location by selecting one of the following buttons:
   - **Add File**: A file is defined by a path, so its security settings will be invalid if that file is moved.
   - **Add Folder Path**: Excludes subfolders, but recursivity may be configured via the registry.
   - **Add Host**: Enter the complete name of the root URL only with no wildcards. For example, www.adobe.com but not www.adobe.com/lc. To specify HTTPS, select **Secure Connections Only**.
3. Choose **OK**.

Figure 10 Enhanced security panel



Specify trusted URLs via Trust Manager

The Trust Manager allows you to permit, block, or be asked about URL access. You may allow or block all URLs, or you can specify a list of trusted URLs. *Trust Manager settings override enhanced security settings*.

Trusting certificates for privileged network operations

When enhanced security is on, a certified document will behave identically to privileged files even if it is not in a privileged location if the following is true:

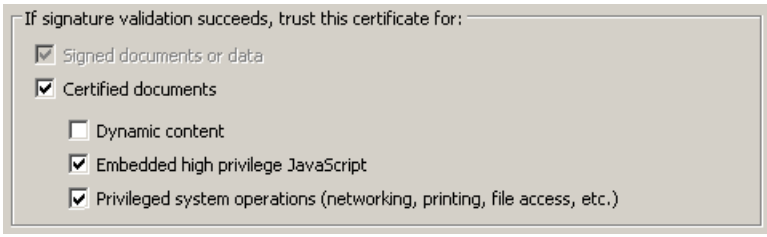
- The document is certified; that is, the first signature in the document is a certification signature.
- The certification signature is valid.
- The document recipient has specifically trusted the signer's certificate for privileged operations.

Post-deployment, administrators can use an FDF file or an acrobatsecuritysettings file to configure the Trusted Identity Manager for multiple clients. Pre-deployment, an administrator would tune the installer with the Acrobat Customization Wizard. For details about certificates, see Digital Signatures and Rights Management in Acrobat and Adobe Reader.

To manually set a certificate's trust level on a client-by-client basis:

1. Choose **Advanced** (Acrobat) or **Document** (Adobe Reader) **> Manage Trusted Identities**.
2. Choose **Certificates** in the **Display** drop down list.
3. Select the certificate.
4. Choose **Edit Trust**.
5. Choose **OK** twice and close the dialog.

Figure 11 Setting certificate trust



Server controls

Managing cross domain access at the server

Clients have the capability of automatically detecting and using crossdomain.xml policy files to access content from a different origin. Administrators can configure the policy file as needed so that clients can access trusted content. For more information, see Cross-domain Access and Configuration.

Enabling cross domain access for specific PDFs

For a PDF that comes from a server, the server has a domain and hence the PDF has a domain; however, a stand-alone PDF residing on a user's machine has no domain. When such a PDF accesses a server, Acrobat's default behavior is to consider that communication as cross domain.

To allow a "domain-less," local PDF to access a server, it must be signed either with a certification signature or a "reader enabled" signature (the hidden signature applied during Reader enablement) and registered in a cross domain policy file. Again, the signature can be one of two types:

- **A certification signature in a certified document**: Best for certified document workflows and when high privileged JavaScript should be permitted.
- **A Reader enabled signature applied by a LiveCycle ES server**: PDFs that are granted additional usage rights are signed by the server. Using this fingerprint allows customers with many Reader extended documents to continue accessing the server after enhanced security is enabled without having to change their forms.

The fingerprint for the certificate that was used for the signing is registered in the cross domain file on the server. In effect, the cross domain file on the server is saying "files signed with this certificate may access this server." To register the fingerprint, an administrator extracts the SHA-1 hash of the public key from the signing certificate and places it in the cross domain policy file. For more information, see Cross-domain Access and Configuration.

Workflow fixes with enhanced security enabled

In most cases, modifying workflows to work with enhanced security enabled is a better choice than disabling the feature. If you experience problems after installing the Acrobat or Adobe Reader 9.3 or 8.2 updates or manually enabling enhanced security, it is a best practice to modify that workflow (See Figure 1).

Here are some common workflow issues caused by a client encountering an untrusted file:

- Form data disappears on form reload after assigning trust via the Yellow Message Bar.

  Tip: If you distribute forms that request data from a server, the user may find that filled formed fields become blank after being asked to trust a document from the Yellow Message Bar. If you don't have direct access to the client, choose Case C to solve your problem. See Case C: You control the application server, but not the clients.

- Script and/or data injection is blocked.
- FDF, XFDF, XDP data cannot be accessed; for example, when a form tries to load data from server.
- Trying to access an item in another domain fails.
- A Yellow Message Bar appears with a security warning.

Case A: You control both the server and clients

In this case, you have the most options:

- Preconfigure clients by assigning trust to a requisite file, folder, or host.
- Have users set privileged locations the on-the-fly via the Yellow Message Bar Options button. Users can assign trust by choosing the **Options** button and trusting the document once or always.
- Place a cross domain policy file on the server and assign trust to hosts, subdomains, and/or documents (such as certified FDFs identified by a certificate fingerprint).
- Set up a certified document workflow, and distribute a trust anchor trusted for privileged networked operations.

Case B: You control the client but not the application servers

- Preconfigure clients by assigning trust to a requisite file, folder, or host.
- Have users set privileged locations the on-the-fly via the Yellow Message Bar Options button. Users can assign trust by choosing the **Options** button and trusting the document once or always.
- Set up a certified document workflow, and distribute a trust anchor trusted for privileged networked operations.

Case C: You control the application server, but not the clients

- Place a cross domain policy file on the server and assign trust to hosts, subdomains, and/or documents (such as certified FDFs identified by a certificate fingerprint).

Case D: You do not control neither the server nor the clients

Provide instructions in the document that will help the user configure their application or make the right choice when trusting content on-the-fly via the Yellow Message Bar Options button. You can have users set privileged locations prior to interacting with documents, or you can set up certified document workflows where end users trust the signing certificate for privileged networked operations.

You already trust certain sites in the browser and want to leverage that trust

For those that already have configured Internet Explorer trusted site lists, configure clients (or instruct users to configure their clients) to trust the Windows OS trusted site list. These sites then become automatically recognized as privileged locations and clients use the union set of the two lists.

Additional resources

For details about enhanced security and cross-domain access, refer to the documents inTable 1.

Table 1 Related Resources

Document	Description
Enhanced Security and Trusted Locations	A guide for configuring enhanced security and trusted content on the client.
Cross-domain Access and Configuration	A technical guide client and policy file configuration.
Cross-domain Policy File Specification	A specification for Acrobat/Reader-compatible X-domain policy files.
Application Security Library	A complete listing of technical guides, quick keys, and other documents.