



## Adobe Approved Trust List - User FAQ

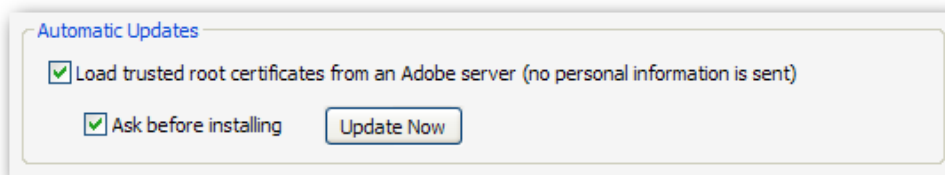
### What is the Adobe Approved Trust List (AATL)?

The Adobe Approved Trust List is a program that allows millions of users around the world to create digital signatures they know will be trusted whenever the signed document is opened in Acrobat or Reader 9.0 and above. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted 'root' digital certificates. Any digital signature created with a credential that can trace a relationship ('chain') back to the high assurance, trustworthy certificates on this list will be trusted by Acrobat and Reader 9.0 and above.

### How do I start using the AATL?

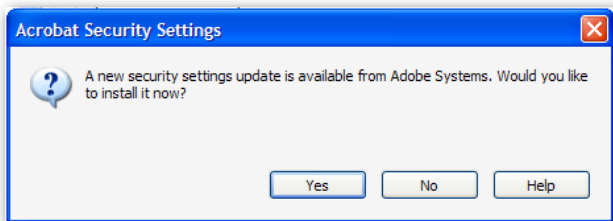
If you're using Acrobat or Reader 9, you don't need to do anything! This feature is turned on by default when you install these products, and the Trust List will automatically be updated every 90 days, though you must open a signed document or open a signature-related menu item to trigger the timer and update.

If you want to verify that the Trust List is enabled, go to Edit (Windows) / Acrobat (Mac) > Preferences->Trust Manager and be sure that the "Load trusted root certificates from an Adobe server..." check box is checked. You can click the "Update Now" button in that same dialog box to download the latest version of the Trust List from Adobe.

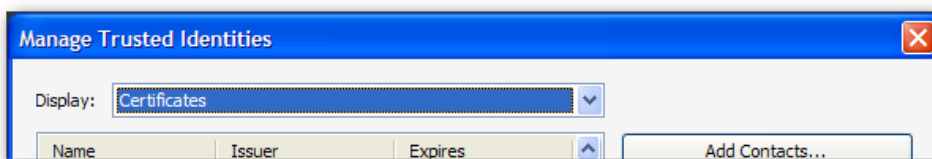


### How do I know if an update is successful?

When the update is ready, you will be prompted with a dialog box like the one below. When you click "Yes," the update happens automatically behind the scenes.

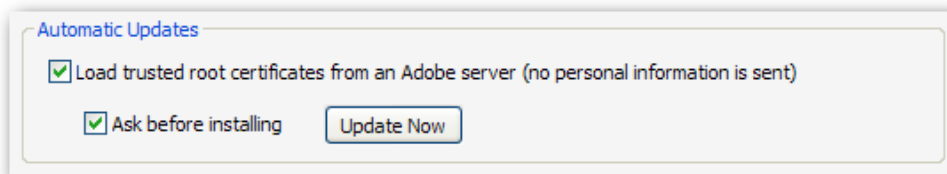


You can check that the update was successful by trying the sample documents available [here](#) or by clicking on Advanced (Acrobat) / Document (Reader)->Manage Trusted Identities, dropping down the box near "Display:" to look at "Certificates," and verify the certificates there include the ones listed on [this webpage](#).



### **I haven't been prompted to update my security settings? Am I doing something wrong?**

Probably not! If you often open signed PDF documents, or have opened even one in the past 90 days, it's possible that the update timer is already counting down, and you're in-between update cycles. Not to worry-- if you want to verify that the Trust List is enabled, go to Edit (Windows) / Acrobat (Mac)->Preferences->Trust Manager and be sure that the "Load trusted root certificates from an Adobe server..." check box is checked. You can click the "Update Now" button in that same dialog box to download the latest version of the Trust List from Adobe.



### **Does Adobe supply AATL credentials / certificates?**

No, Adobe does not provide AATL-based credentials for purchase. Adobe works with leading CAs and governments from around the world to provide trust in its products for these certificates. If you'd like to purchase an AATL-based certificate, please contact one of the certificate authorities listed on the [AATL webpage](#). You also may be eligible for, or already have, an AATL-enabled

certificate if your national / federal identity credentials come from one of the AATL Members listed on the [AATL webpage](#).

### **What version of Acrobat or Reader do I need to be running?**

You will need version 9.0 or above of Acrobat or Reader to *validate* signatures based on AATL credentials. You can *sign* with an AATL credential in earlier versions of these products, but the trust inherent in AATL will only be visible in version 9.0 and above of Acrobat and Reader.

### **How is the Adobe Approved Trust List different from the Certified Document Services (CDS) program?**

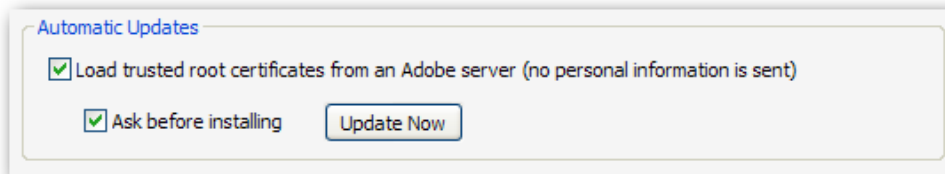
The AATL complements our existing Certified Document Services (CDS) trust program, where new digital IDs that are chained to the Adobe Root certificate embedded in Adobe products are automatically trusted. CDS is key to document certification efforts at the [US Government Printing Office](#), [Avow Systems](#), the [Antwerp Port Authority](#), and many other customers who use high assurance signatures to protect the integrity and authorship of key electronic documents. Anybody who opens a PDF document signed or certified by a CDS credential automatically gets a 'blue ribbon' experience with trust provided to the signature without any user interaction. CDS credentials are backwards compatible from the current generation of Acrobat and Reader all the way back to version 6. Five [certificate authorities](#) currently offer CDS certificates.

While the high level benefits of the Adobe Approved Trust List program are similar, the AATL is only available in Acrobat and Reader 9 at this time. It is not backwards compatible. However, existing certificate communities, such as government national ID card programs, can join the AATL, as the chain to the Adobe Root certificate is not required. On the other hand, all CDS Providers offer certificates that meet a high standard for assurance and feature additional capabilities including the embedding of robust timestamping and real-time revocation to provide for long term validation of digital signatures. Contact Adobe to get more information about which program is right for your organization / government.

### **Can I turn the AATL off?**

While the AATL update capability is turned on by default to promote trust in high assurance signing credentials, it is possible to turn it off. An individual user can go to Edit (Windows) / Acrobat (Mac)->Preferences->Trust Manager and click to clear the checkbox next to "Load

trusted root certificates from an Adobe server..." and then click OK. Enterprises and organizations can also turn off this capability via registry changes or other methods described in [this document](#).

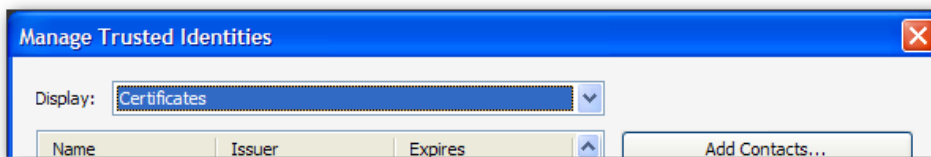


Are there any sample documents I can try to test whether the AATL update was successful?

Yes, visit the AATL webpage [here](#) to find sample documents.

How can I find out which organizations are included in the AATL?

The [AATL home page](#) lists the latest organizations and certificates included in the AATL. You can also click on Advanced (Acrobat) / Document (Reader)->Manage Trusted Identities, dropping down the box near "Display:" to look at "Certificates," and see the certificates listed there.



Why is the AATL important?

When you receive a digitally signed document, both Reader and Acrobat ask three key questions to validate the signature.

1. Is the digital certificate that signed the document still valid? Has it expired or been revoked?
2. Has the document been changed since it was signed? Has the integrity of the document been affected? If there are changes, are they allowed changes or not allowed changes?
3. Finally, does this certificate chain up to a certificate listed in the Trusted Identity list? If so, the signature will be trusted automatically.

The answers to the first two questions are handled by Acrobat and Reader based on an analysis of the information contained within the certificate and the signed document itself. However, it's the answer to the third question which has always posed a challenge for the electronic signatures marketplace.

How do you know to trust a digital signature? What aspects of the signer's digital certificate / credential should be noted? How important is identity verification prior to granting of the digital certificate to the signer, and how critical is the storage of the signing key itself?

Adobe understands that the relying party must be free to make their own trust decisions based on their own unique circumstances. If Adobe were to trust every signature credential, users might accept signatures from false identities or trust documents that should not be trusted in the first place. Adobe products feature several different ways in which to set this trust, and the AATL is the latest method by which we are making this easier.

### **Why can't I just go in and trust all of the certificates in the Windows Certificate Store?**

In order to best serve the purposes of web browsing, operating system and browser vendors have created lists of trusted identities (SSL certificates) to enable more secure transactions online. Users of Adobe products have the option to allow the software to trust all of the certificates in the Windows Certificate Store, though this option is not selected by default. Why? Adobe believes the store casts too wide a net, and trusts a large number of both high and low assurance certificates, thereby introducing unnecessary risk into a document signing scenario. The rise of the enhanced validation (EV) SSL certificate also highlights this problem.

In any case, you can certainly enable this option, as there may be viable reasons for you to do so. However, be sure to understand the implications.

### **How do I get an AATL credential?**

If you'd like to purchase an AATL-based certificate, please contact one of the certificate authorities listed on the [AATL webpage](#). You also may be eligible for, or already have, an AATL-enabled certificate if your national / federal identity credentials come from one of the AATL Members listed on the [AATL webpage](#).

## How can I set up trust for other certificates and organizations?

If you are interested in either manually setting trust for other certificates, or your enterprise is interested in ways to automate this, please read the following blog entries at [Security Matters](#), and then take a look at [this document](#) for more details.

- [Setting Signature Trust in Adobe Products Part 1](#)
- [Setting Signature Trust in Adobe Products Part 2](#)
- [Setting Signature Trust in Adobe Products Part 3](#)

## How does the AATL work?

Certificate authorities (CAs), entities which provide digital signing credentials to other organizations and end users, as well as governments / organizations that provide certificates to their citizens & employees, can apply to Adobe to join the AATL program by submitting application materials and their root certificate (or another qualifying certificate). After verifying that the applicant's services and credentials meet the assurance levels imposed by the AATL Technical Requirements, Adobe adds the certificate(s) to the Trust List itself, digitally signs the Trust List with an Adobe corporate digital ID that is linked to the Adobe Root certificate embedded in Adobe products, and then posts the List to a website hosted by Adobe.

[Adobe products which support the AATL](#) will automatically download this file every 90 days, though you must open a signed document or open a signature-related menu item to trigger the timer and update.. Before the contents are deposited into the client's Trusted Identity list, the list is verified to ensure it came from Adobe.

## Why is my default setting different from the instructions?

It's possible that your organization has changed the default settings in Acrobat or Reader based on the specific needs of your IT environment. Please contact your IT administrator for more information.

## Does the AATL allow me to sign documents in Reader?

No, not by itself. Signing in Reader is only possible if you are opening a document that has been 'extended' (that is, enabled) for signing in Reader via Acrobat's "Extend Features in Adobe Reader" capability or via LiveCycle Reader Extensions server, usually by the author of the document.

You can sign PDF documents in Acrobat, however.

### **Can I modify or delete the certificates in the AATL?**

Once the AATL update is complete, and the certificates appear in your "Manage Trusted Identities" dialog box, then yes, you can modify the trust for each of the certificates, or outright delete some of them, if you wish. Note that these certificates may re-appear during the next update cycle of the AATL, so you would have to manually modify them again.

### **Where can I go to get more information about the AATL?**

Please visit the AATL home page [here](#).