



PDF Creation Date:

December 8, 2006

Sharing Acrobat Settings and Data with FDF Files

Acrobat® and Adobe® Reader®

Version 8.X

© 2006 Adobe Systems Incorporated. All rights reserved.

As of April 12, 2002, Accelio Corporation (formerly JetForm Corporation) was purchased by Adobe Systems Incorporated. As of that date, any reference to JetForm or Accelio shall be deemed to refer to Adobe Systems Incorporated.

Sharing Acrobat Settings and Data with FDF Files.

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Any references to company names in sample templates are for demonstration purposes only and are not intended to refer to any actual organization.

Adobe, Acrobat, Reader, and the Adobe logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Windows, Windows NT, and Windows XP are registered trademarks of Microsoft Corporation registered in the United States and/or other countries. Mac and Macintosh are registered trademarks of Apple Computer, Inc. in the United States and other countries. All other trademarks are the property of their respective owners.

All other trademarks are the property of their respective owners.

Adobe Systems Incorporated, 345 Park Avenue, San Jose, California 95110, USA.

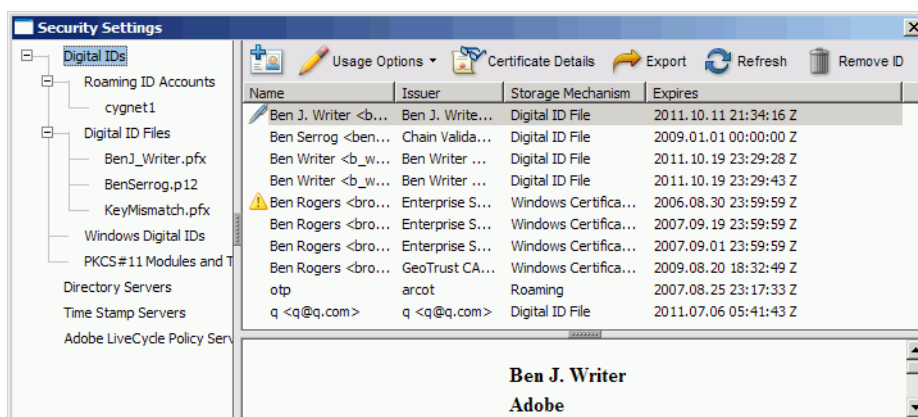
Notice to United States Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States. Adobe Systems Incorporated, 345 Park Avenue, San Jose, CA 95110-2704, USA. For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Sharing Application Settings & Digital IDs with FDF

Acrobat and Adobe Reader use FDF files to exchange data between the Acrobat family of client and server products. FDF files use a .fdf extension, and like .pdf, it is registered by Adobe so that files with these extensions are opened by the required application when opened in a browser or file explorer.

With FDF files, users can exchange digital ID certificates as well as server settings for an Adobe Policy Server, LDAP directory servers, roaming credential servers, and timestamp servers. FDF files can be created on a server or by users. The files can be shared in networked directories or sent as email attachments. Data is exported and imported from the Security Settings user interface, and many items in the left-hand tree provide **Import** and **Export** buttons in the top-level menu (Figure 1).

Figure 1 Security Settings menu items



Individual users can share digital ID certificates and server data while administrators can distribute FDF files across an organization's users to configure and update client installations. Whether the file is located on a network or emailed, FDF file recipients simply double click on a FDF file to import its data automatically via the FDF import wizard, thereby eliminating the need for error prone, manual configuration.

FDF files provide individuals and businesses with many opportunities for streamlining workflows. For example:

- Alice wants to email her certificate to Bob and wants Bob to reply with his certificate. Alice chooses **Request Contact** in the Trusted Identity Manager. The workflow generates and emails an FDF file that can contain her certificate, a request for Bob's certificate, and Alice's return email address.
- Alice needs to encrypt documents for a number of people in her organization. An administrator sends her an FDF file that contains a large group of contacts. When Alice opens the FDF file, she is walked through the FDF Data Exchange UI wizard so that she can import these contacts into her Trusted Identities list.
- A server wants a copy of Bob's certificate so that the server can encrypt documents for Bob. The server generates an FDF file that contains a certificate request and a return URL address. When Bob's downloads the FDF file from the server, he is walked through the FDF Data Exchange UI wizard where he can respond by allowing his certificate to be returned.
- A company needs to distribute its trusted certificate to customers so that they can verify that the company's documents are authentic. A server or administrator creates an FDF file that contains the trusted certificate and posts it on a Web server that hosts a Web page with a link to the file. When customer's download the file, they are asked whether they wish to add this certificate to the Trusted Identity list and are given the ability to set the certificate's trust level.

For more information, refer to the following:

- [Importing Application Settings and Digital ID Data](#)
 - [“Responding to an Emailed Request for a Digital ID” on page 5](#)
 - [“Importing Someone’s Certificate” on page 6](#)
 - [“Importing Multiple Certificates” on page 7](#)
 - [“Importing Timestamp Server Settings” on page 9](#)
 - [“Importing Directory Server Settings” on page 10](#)
 - [“Importing Adobe Policy Server Settings” on page 11](#)
 - [“Importing Roaming ID Account Settings” on page 13](#)
- [Exporting Application Settings and Digital ID Data](#)
 - [“Distributing a Trust Anchor or Trust Root” on page 18](#)
 - [“Exporting Your Certificate” on page 21](#)
 - [“Requesting a Certificate via Email” on page 24](#)
 - [“Emailing Server Details” on page 25](#)
 - [“Exporting Server Details” on page 26](#)

Importing Application Settings and Digital ID Data

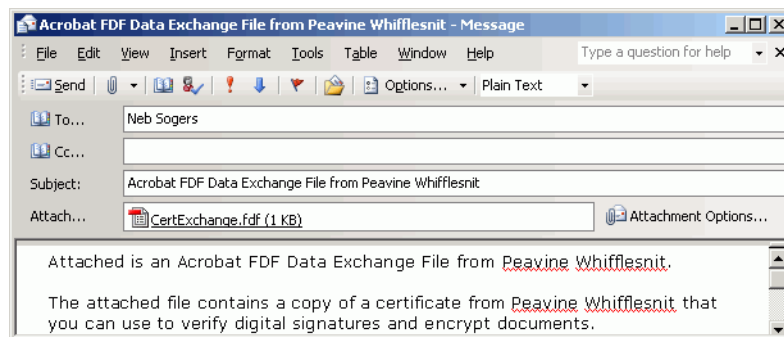
There are several ways to import Acrobat and Adobe Reader data from an FDF file:

- By choosing **File > Open**.
- Double clicking on an FDF file (.fdf)

Tip: The first two options above automatically invoke the correct workflow.

- For digital ID information, importing it into the Trusted Identity Manager.
- For server settings, importing it with the Security Settings dialog.

Figure 2 FDF Email attachment



Responding to an Emailed Request for a Digital ID

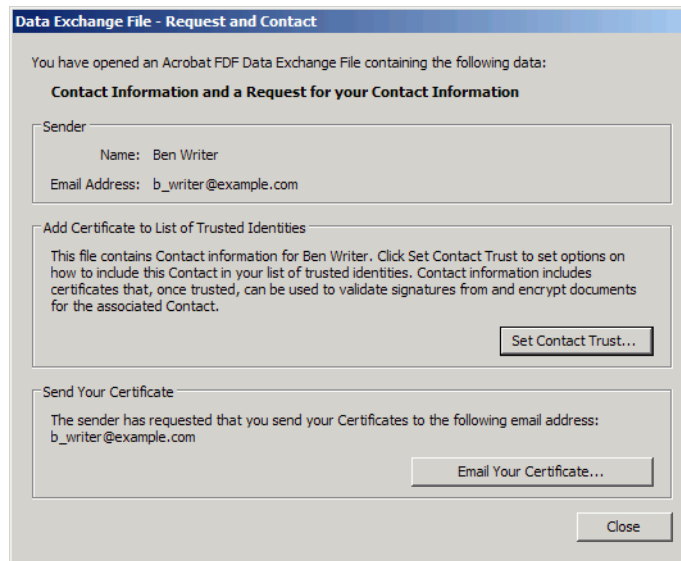
There may be times when someone else needs your digital ID to verify your signature or encrypt a file for you to decrypt (apply certificate security). To do either, they need access to the public part of your digital ID so that it can be added to their trusted identities list. One way someone can get your ID is to request it in an email.

To request your certificate, a user will simply choose **Advanced > Manage Trusted Identities** and then choose **Request Contact**. Acrobat automatically attaches an FDF file with their public digital ID information to an email that requests your digital ID. The workflow is essentially a digital ID "trade" that allows two users to exchange digital IDs. You must have a digital ID before responding to the request.

To respond to an emailed digital ID request:

1. Double click the attached FDF file.
2. Choose **Email your Certificate**.

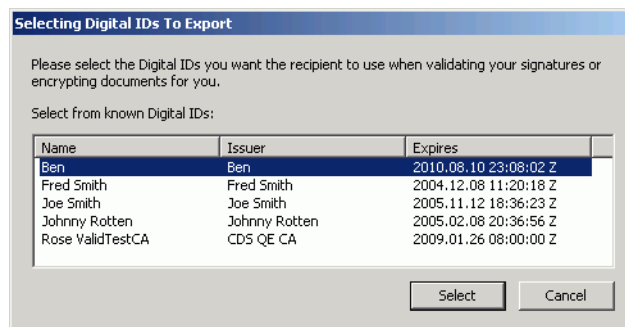
Figure 3 Emailing your certificate



3. Choose a digital ID from the list of existing digital IDs.

Note: If you do not have a digital ID or choose **Cancel**, an alert appears that says "A certificate was not selected for export." Exit the workflow and get a digital ID.

Figure 4 Selecting a digital ID



4. Choose **Select**.
5. Review the email details. You can edit the To, Subject, and Body fields.
6. Choose **Email**.
7. Send the email through your mail application.

Importing Someone's Certificate

You can use an FDF file to import someone's certificate into your list of trusted identities. This enables you to validate their signature and encrypt documents with their public key so only that intended recipient can open it.

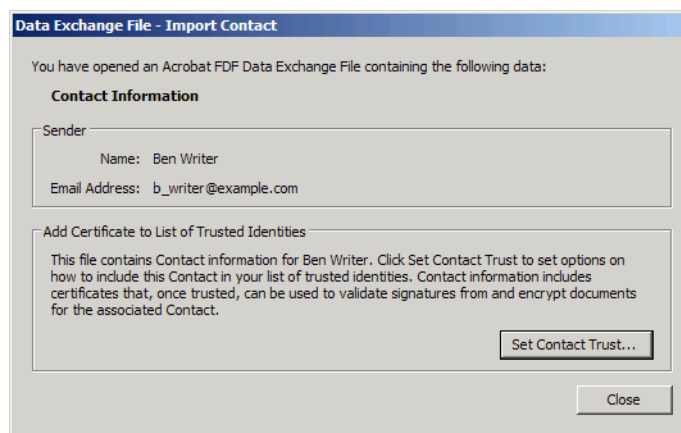
Tip: Importing this information ahead of time enables you to configure your trusted identities list before needing to validate a signature or encrypt a document for someone.

To add someone's certificate to your list of trusted identities:

1. Click on the FDF file or from Acrobat or Adobe Reader choose **File > Open**. The digital ID certificate may be sent directly from Acrobat as an email attachment (Figure 2) or may reside in a networked directory.
2. Review the sender's information when the Import Contact dialog appears.

Note: If the file is signed, then the Import Contact dialog will also have a Signature panel as shown in Figure 6.

Figure 5 Certificates: Contact Information



3. Choose **Set Contact Trust**.
4. When the Import Contact Settings dialog appears, configure the Trust and Policy Restrictions. For details, see ["Importing a Trust Anchor and Setting Trust" on page 14](#).
5. Choose **Certificate Details**.
6. Choose the Details tab.
7. In the Certificate data panel, scroll to MD5-digest and SHA-1 digest and note the fingerprint numbers.
8. Contact the certificate's originator and verify the fingerprints are correct.
9. Choose **OK**.
10. Choose **OK**.
11. Choose **Close**.

Importing Multiple Certificates

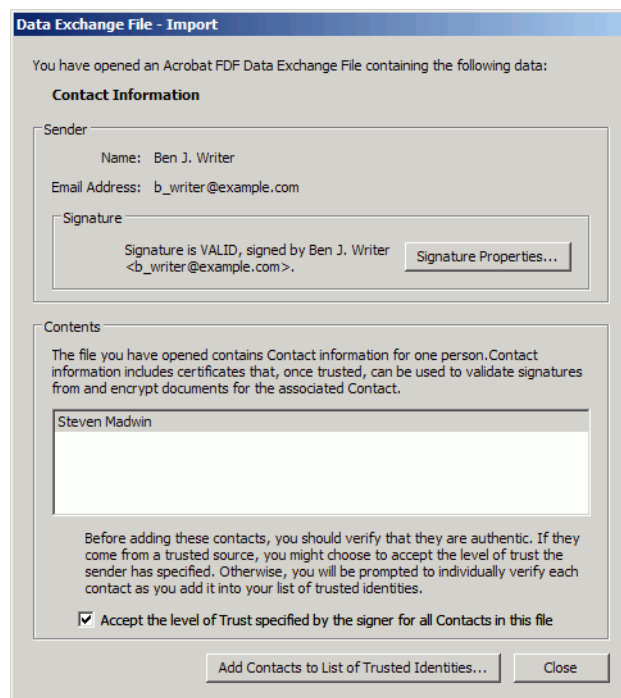
You can use an FDF file to import multiple certificates or a company-wide address book into your list of trusted identities. This enables you to encrypt documents with their public key so only that intended recipient can open it.

Tip: Importing this information ahead of time enables you to configure your trusted identities list before needing to validate signature or encrypt a document to those identities. Administrators can create a company-wide address book and can export it to an FDF file for distribution throughout a company via a network or email.

To add multiple certificate to the trusted identities list all at once:

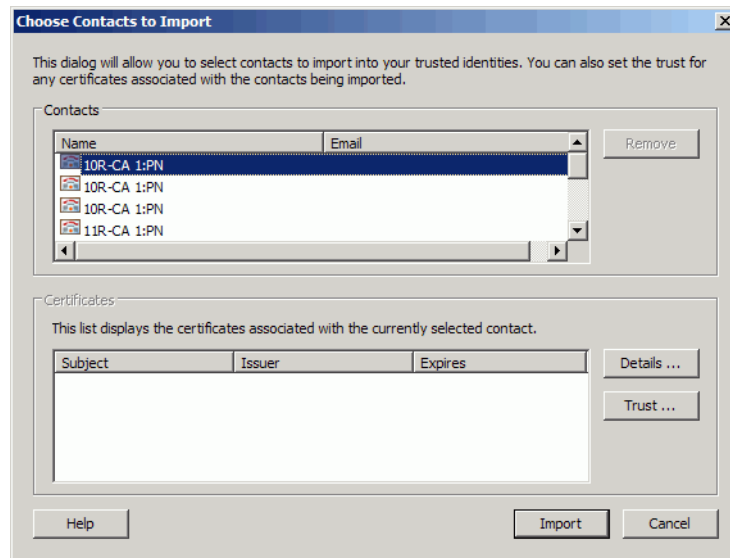
1. Click on the FDF file or from Acrobat or Adobe Reader choose **File > Open**. The digital ID certificate may be sent directly from Acrobat as an email attachment (Figure 2) or may reside in a networked directory.

Figure 6 Importing multiple certificates



2. If the FDF file is signed AND a trust level has been specified by the sender, check or uncheck **Accept the level of Trust specified by the signer for all Contacts in this file**.
 - If the checkbox is selected, all contacts associated with this certificate will accept the level of trust that was set by the user that signed the FDF file.
 - If the checkbox is not selected, no trust level will be set for these certificates. The certificate cannot be used for many actions (such as providing a valid timestamp or encrypting) until a trust level is set as described in the user documentation.
3. Choose **Add Contacts to List of Trusted Identities**.
4. If there are multiple contacts in the file, the Choose Contacts to Import dialog appears. Remove those that are not wanted and highlight the rest.
5. Choose **Import**.
6. Choose **OK** in the confirmation dialog.

Figure 7 Making a contact a trusted identity



Importing Timestamp Server Settings

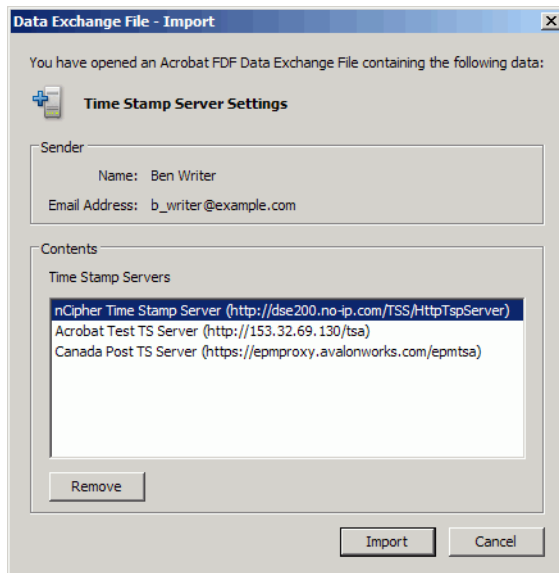
In enterprise settings, these servers do not usually have to be manually configured. Timestamp server administrators often export the server information to an FDF file which is emailed or made available on a network. Users can import (add) directory server settings through the Security Settings user interface or simply by double clicking on the FDF file containing the data.

To import the server settings:

1. Locate the FDF file: find the file in an email or on the local file system and double click on it.
The FDF can also be imported through the Security Settings dialog by choosing **Advanced > Security Settings**, selecting **Time Stamp Servers** in the left-hand list, and choosing **Import**.
2. Review the sender's details. Verify the signature properties if needed (Figure 8).

Note: If the FDF is not signed, the Signature panel will display *Not signed* and the **Signature Properties** button will be disabled.

Figure 8 Timestamps: Importing server details from an FDF file



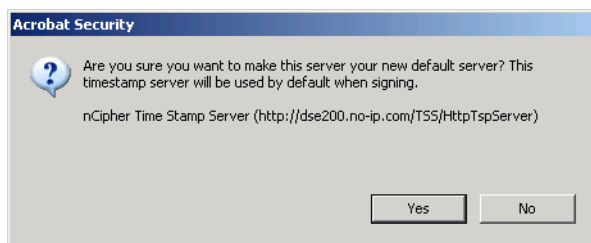
3. Review the timestamp server list.

Note: If there is more than one server and you do not want to import all of them, highlight those that should not be imported and **Select Remove**.

4. Choose **Import**.

A dialog appears asking if the first (or only) server in the server list should be used as the default.

Figure 9 Timestamps: Importing a default server



5. Choose **Yes** or **No**.

If **No** is selected, a default timestamp server must be set before timestamps can be used. To set a default timestamp server, Choose **Advanced > Security Settings > Time Stamp Servers**, select a server, and choose **Set Default**.

6. After the import completes, choose **OK**.

The settings are automatically imported and should now appear in your list of Time Stamp Servers.

Importing Directory Server Settings

In enterprise settings, these servers do not usually have to be manually configured. Server administrators often export the server information to an FDF file which is emailed or made available on a network. Users

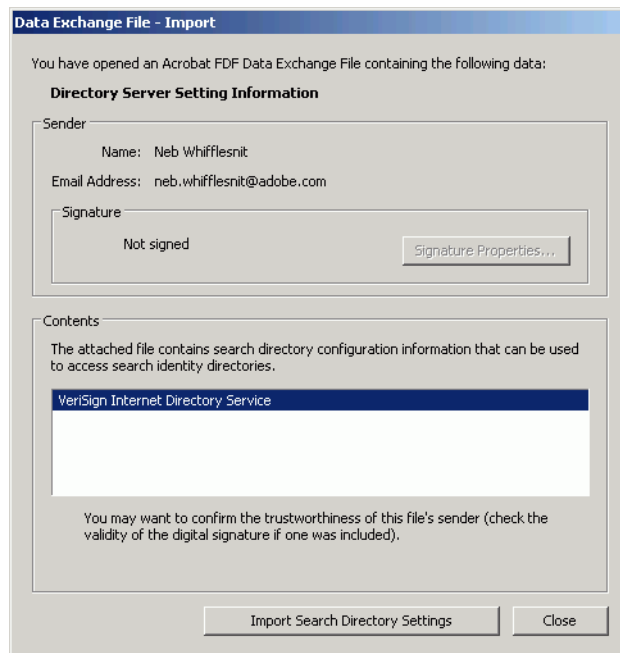
can import (add) directory server settings through the Security Settings user interface or simply by double clicking on the FDF file containing the data.

To add server settings from a file:

1. Locate the FDF file: find the file in an email or on the local file system and double click on it.
The FDF can also be imported through the Security Settings dialog by choosing **Advanced > Security Settings**, selecting **Directory Servers** in the left-hand list, and choosing **Import**.
2. Review the sender's details. Verify the signature properties if needed (Figure 10).

Note: If the FDF is not signed, the Signature panel will display *Not signed* and the **Signature Properties** button will be disabled.

Figure 10 Digital ID Directory servers: Importing



3. Choose **Import Search Directory Settings**.
4. If a confirmation dialog appears, choose **OK**.
This dialog will not appear if **Do not show this message again** was previously selected.
5. Choose **Close**.
The settings are automatically imported and should now appear in the Directory Servers list in the Security Settings dialog.

Importing Adobe Policy Server Settings

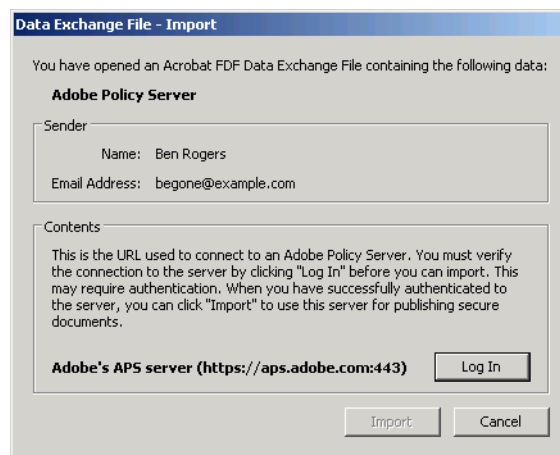
In enterprise settings, these servers do not usually have to be manually configured. APS administrators often export the server information to an FDF file which is emailed or made available on a network. Users can import (add) directory server settings through the Security Settings user interface or simply by double clicking on the FDF file containing the data.

To import the server settings:

1. Locate the FDF file: find the file in an email or on the local file system and double click on it.
The FDF can also be imported through the Security Settings dialog by choosing **Advanced > Security Settings**, selecting **Adobe Policy Servers** in the left-hand list, and choosing **Import**.
2. Review the sender's details. Verify the signature properties if needed (Figure 10).

Note: If the FDF is not signed, the Signature panel will display *Not signed* and the **Signature Properties** button will be disabled.

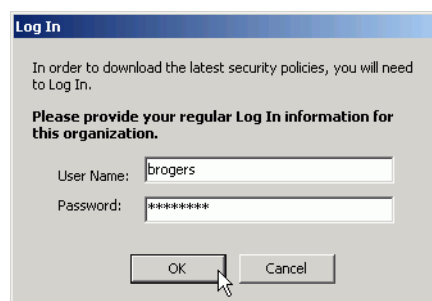
Figure 11 Importing APS settings



3. Choose **Log In**.

Tip: You must identify yourself to the server before you will be allowed to import these settings. The Import button does is disabled until you log in.

Figure 12 Logging in to an Adobe Policy Server



4. Choose **OK**.
5. Choose **Import**.
6. If you do not already have a default Adobe Policy Server, a dialog appears asking whether or not you want to make this your default server, choose **Yes** or **No**.

7. Choose **OK**.

The settings are automatically imported and should now appear in the Adobe LiveCycle Policy Servers list in the Security Settings dialog.

Importing Roaming ID Account Settings

In enterprise settings, these servers do not usually have to be manually configured. Roaming ID server administrators often export the server information to an FDF file which is emailed or made available on a network. Users can import (add) directory server settings through the Security Settings user interface or simply by double clicking on the FDF file containing the data.

To import the server settings:

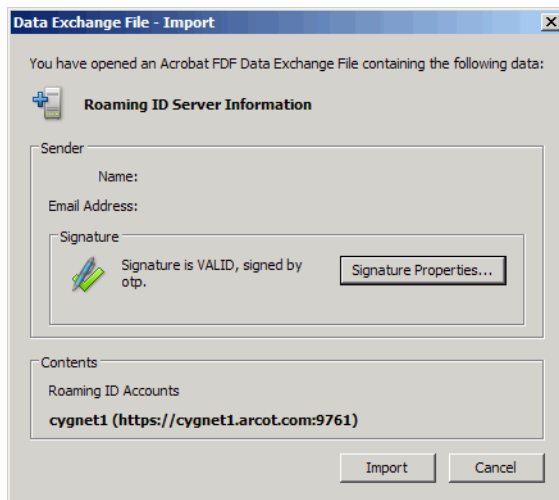
1. Locate the FDF file: find the file in an email or on the local file system and double click on it.

The FDF can also be imported through the Security Settings dialog by choosing **Advanced > Security Settings**, selecting **Roaming ID Accounts** in the left-hand list, and choosing **Import**.

2. Review the sender's details. Verify the signature properties if needed (Figure 13).

Note: If the FDF is not signed, the Signature panel will display *Not signed* and the **Signature Properties** button will be disabled.

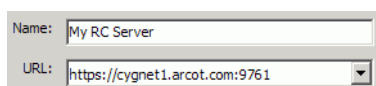
Figure 13 Importing roaming ID server settings



3. Choose **Import**.

4. Verify the roaming ID account name and server URL.

Figure 14 Roaming ID server name and URL

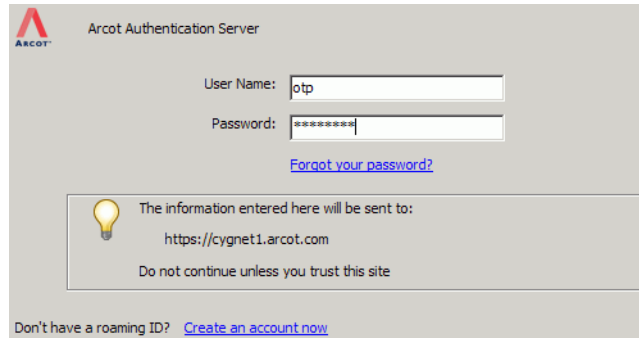


5. Choose **Next**.

6. Enter a user name and password.

Tip: The topmost portion of this dialog is customizable and server-dependant. The fields will remain the same, but the branding will vary.

Figure 15 Logging in to a roaming ID server



7. Choose **Next**.
8. After the confirmation that you have downloaded the roaming ID(s) appears, choose **Finish**.
The server settings and associated certificates are automatically imported and will now appear in the Roaming ID Accounts list in the Security Settings dialog.

Figure 16 Downloaded roaming ID certificates

You have downloaded the following roaming ID(s):

Name	Issuer	Expires
otp	arcot	2007.08.25 23:17:33 Z

Importing a Trust Anchor and Setting Trust

Users occasionally need to import a trust anchor into their trusted identities list so that certificates that chain up to that anchor will also be trusted. This is particularly true in large organizations, and system administrators often distribute a trust anchor so that everyone within that organization can trust everyone else at the same level for signature workflows.

To import a certificate that will be used as a trust anchor:

1. Open the FDF with one of the following methods:
 - Click on the FDF file. It may be an email attachment or a file on a network or your local system.
 - In Acrobat or Adobe Reader choose **File > Open**, browse to the FDF file, and choose **Open**.

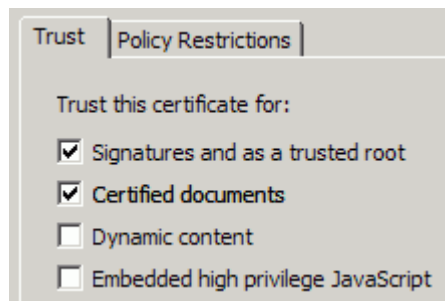
Note: It is unlikely that you will receive a signed FDF file containing a trusted root. However, if you do, simply check **Accept the level of trust specified by the signer for all contacts in this file** and then choose **Close**. The rest of the following steps may be skipped.

2. For unsigned FDF files containing a trusted root (the most likely case), choose **Set Contact Trust**.

1. Do one of the following:
 - If you already have the certificate,
 1. Choose **Advanced > Manage Trusted Identities**.
 2. Choose **Certificates** in the **Display** drop down list.
 3. Select the certificate.
 4. Choose **Edit Trust**.
 - If the certificate is in a signature,
 1. Right click and choose **Signature Properties**.
 2. Choose **Show Certificate**.
 3. Select the Trust tab.
 4. Choose **Add to Trusted Identities**.
5. On the Trust tab, select the requisite trust options.

Note: In enterprise settings, the administrator should tell you which trust settings are appropriate.

Figure 17 Certificate trust settings



- **Signatures and as a trusted root:** Trusts the certificate as a trust anchor. The net result is that any certificates which chain up to this one will also be trusted for signing. At least one certificate in the chain (and preferably only one) must be a trusted root (trust anchor) to validate signatures and timestamps certificates.

Tip: There is no need to make end entity certificates trusted roots if they chain up to a trust anchor. It is best practice to trust the topmost certificate that is logically reasonable to trust because revocation checking occurs on every certificate in a chain until that anchor is reached. For example, in a large organization, it is likely you would want to trust your company's ICA certificate. If that certificate chains up to VeriSign, you would not want to make VeriSign a trusted root unless you wanted to trust every certificate that chains up to VeriSign.

- **Certified Documents:** Trusts the certificate for certification signatures.
- **Dynamic Content:** Trusts movies and other dynamic content. This option requires that the application environment be configured correctly.

Caution: This option interacts with other settings as described in [“Setting Multimedia Trust Levels” on page 196](#).

- **Embedded High Privilege JavaScript:** Trusts embedded scripts. This option requires that the application environment be configured correctly.

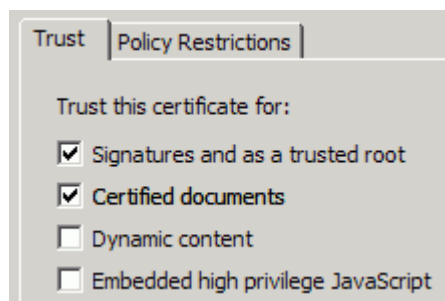
Caution: This option interacts with other settings as described in [“Setting High Privilege JavaScript Security Options” on page 198](#).

Note: Recipients of the distributed root will be able to inherit these trust settings as well as any other trust settings of certificates higher up in the chain during import.

6. If you need to specify a policy restriction, do so. Most users do not need to set policy restrictions or only do so at the request of their administrator.
7. Choose **OK** twice.
8. Choose **Close**.
9. On the Trust tab, select the requisite trust options.

Note: In enterprise settings, the administrator should indicate which trust settings are appropriate.

Figure 18 Certificate trust settings



10. Configure the Trust tab:

- **Signatures and as a Trusted Root:** Trusts the certificate as a trusted root for approval signatures. The net result is that any other certificates which have this one as a root in the chain will also be trusted for signing. At least one certificate in the chain (and preferably only the root in the chain) must be a trusted root to validate signatures and timestamps certificates.

Tip: There is no need to make end entity certificates trusted roots if they chain up to a trust anchor. It is best practice to trust the topmost certificate that is logically reasonable to trust because revocation checking occurs on every certificate in a chain until that anchor is reached. For example, in a large organization, it is likely you would want to trust your company’s ICA certificate. If that certificate chains up to VeriSign, you would not want to make VeriSign a trusted root unless you wanted to trust every certificate that chains up to VeriSign.

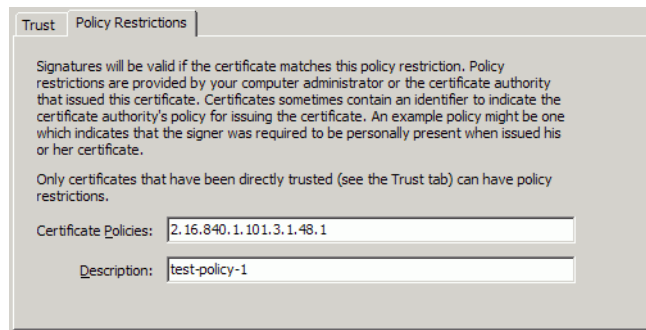
- **Certified Documents:** Trusts the certificate for certification signatures.
- **Dynamic Content:** Trusts movies and other dynamic content. This option requires that the application environment be configured correctly.
- **Embedded High Privilege JavaScript:** Trusts embedded scripts. This option requires that the application environment be configured correctly.

Note: Recipients of the distributed root will be able to inherit these trust settings as well as any other trust settings of certificates higher up in the chain during import.

11. Configure the Policy Restrictions tab:
 - **Certificate Policies:** Enter the policy OID.
 - **Description:** Enter a meaningful description.

Tip: Policy restrictions are typically used in enterprise settings when configuring trust anchors. A restriction provides additional criteria the certificate chain must meet before a signing certificate can be used to create a valid signature. For example, a VeriSign certificate may be set as a trusted root, but a company may wish to only trust their own intermediate certificates (ICA) that chain to VeriSign rather than all certificates that chain up to VeriSign. The company can issue an ICA with a certificate policy extension. By including that ICA in the certificate chain between all end entity certificates and VeriSign and requiring the presence of that extension in Acrobat, only company signers will be trusted.

Figure 19 Policy restrictions



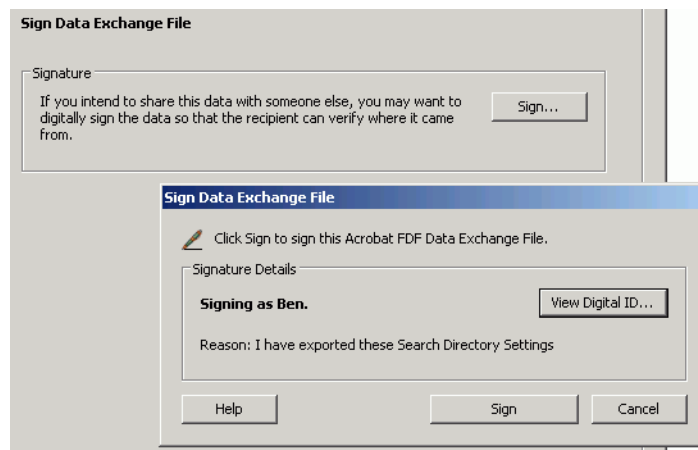
12. Choose **OK**.
13. Choose **OK**.
14. Choose **Close**.

Exporting Application Settings and Digital ID Data

FDF files can be created by administrators, end users, and even a server. It is a good idea to sign FDF files so that recipients of the file can establish a level of trust for the contents of the FDF file. For example, when an FDF file is signed, the **Accept the level of trust specified by the signer for all contacts in this file** checkbox becomes enabled, thereby allowing the importer to accept the level of trust you have specified.

Note: Recipients won't be able to validate your signature unless you have previously sent them your digital ID certificate.

Figure 20 Signing an FDF file



Distributing a Trust Anchor or Trust Root

Distributing a trusted certificate from Acrobat involves wrapping one or more certificates in an FDF file and making it available to other users via email, a network directory, or a Web site. Recipients simply click on the file or a link to the file to open the Acrobat wizard which downloads and/or installs the certificate.

Certificate Chains and Trust Anchors /Roots

Certificates usually exist as part of a hierarchy or "chain" of certificates, and part or all of the chain can be wrapped in an FDF file. The bottom-most and end user certificate (yours) is called an "end entity" (EE) certificate. The top-most certificate, (the root) is typically belongs to a trusted Certificate Authority (CA). Certificates in between the end entity and root certificates are sometimes called "intermediate certificates" (ICAs) and are issued by the CA or ICAs underneath the CA. Acrobat enables users to specify one or more of the certificates in a chain as trusted for specific operations. Thus, an EE certificate could have one or more trust anchors (trusted ICAs) that chain up to a the top-most CA certificate which is the primary trust anchor or "trusted root."

A typical chain might include your certificate, your company's ICA, and a root CA. Certificates inherit trust from certificates higher up in the chain. For example, if the root certificate is trusted, then any certificates chaining up to the that root will also be trusted. Some organizations have their own root CA or use an ICA certificate that is issued by an external CA and make these the trust anchors for their employees.

It is a common practice to trust certificates as high up in the chain as is reasonable since revocation checking starts at the chain bottom and continues until it reaches a trust anchor. Revocation checking should occur until reaching a certificate that is absolutely trusted by you or your organization. It also allows users to trust other certificates that chain up to the same root. The trust anchor is often an ICA for

example, since if the root is issued by a company such as VeriSign, it might not be wise to make it a trust anchor as that tells Acrobat to trust the millions of certificates that chain up to VeriSign.

Distributing and installing ICA or CA trust anchors to a user or group of users allows them to:

- Distribute certified or signed documents to partners and customers.
- Help document recipients validate the signatures of document authors.

Export the Trust Anchor

When Acrobat exports a certificate, it automatically exports other selected certificates in that certificate's chain and includes them in the FDF file.

1. Choose **Advanced > Manage Trusted Identities**.

2. Choose **Certificates** in the **Display** drop down list.

In addition to this method, you can also display the certificate from any signature or certificate security method workflow where a **Show Certificate** or **Certificate Details** button appears, such as the Signature Properties dialog.

3. Select the certificate ([Figure 22](#)).

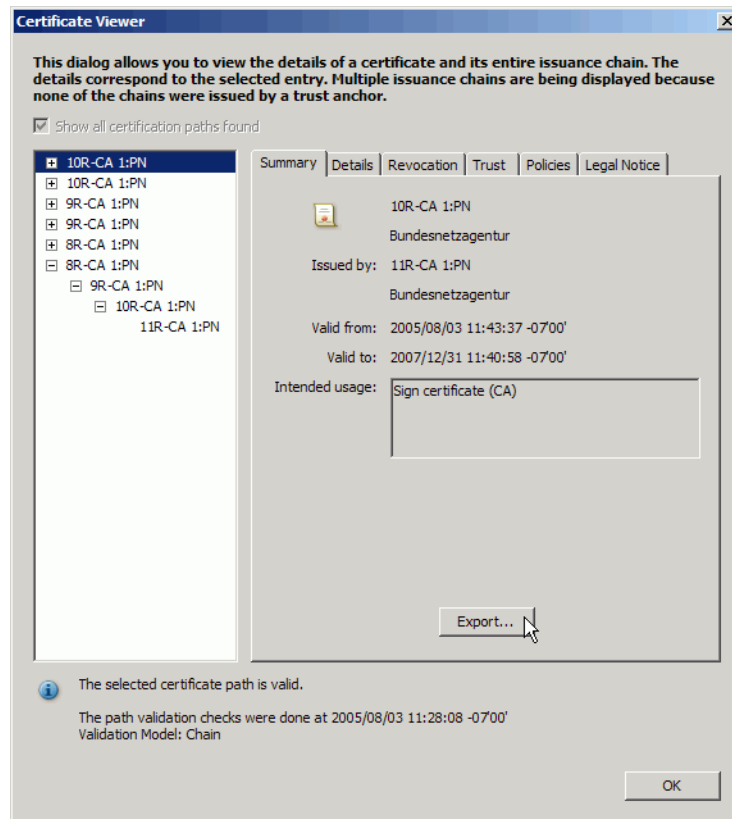
Note: In the unlikely event that you can sign the FDF file with a signature the recipient can validate (they will use a different certificate than the one you are exporting), set the certificate's trust level before exporting it. For details, see "[Optional: Setting Certificate Trust Level](#)" on page 21

Tip: You could just choose **Export** and bypass the following two steps. However, exporting the certificate from the Certificate Viewer allows you to see the entire certificate chain where you can select all or part of it.

4. Choose **Show Certificate**. The Certificate Viewer displays the certificate.

5. Select a certificate in the chain that appears in the left-hand window.

Figure 21 Selecting a certificate chain for export



6. Choose **Export**.
7. Choose one of the following:
 - **Email the data to someone: Emailing the data automatically creates an FDF file that other Adobe product users can easily import.**
 - **Save the exported data to a file: Acrobat FDF Data Exchange. FDF is a format that other Adobe product users can easily import. It is only recognized by Adobe products.**
8. Choose **Next**.
9. **Optional:** If the Identity Information dialog appears, enter the your email address and any other information. If you have already configured your identity details, this screen may not appear. To view your current settings, choose **Edit > Preferences > Identity**.
10. **Do not sign** if the certificate you use to sign uses the same trust anchor or you are distributing. Since recipients do not have this certificate yet, they will not be able to validate your signature.

Note: Signing the FDF will only be useful if you have a digital ID that the recipient has already trusted (uses a trust anchor OTHER than the one you are currently distributing). The FDF file recipients must also already have that digital IDs certificate so that they can validate your signature without relying on the certificate you are currently sending. This workflow is uncommon, but it does allow recipients to automatically inherit your predefined trust settings for the certificate embedded in the file.
11. Choose **Next**.

12. Continue with the workflow until the trusted root is emailed or placed in a directory where your intended recipients can find it.

Provide Instructions to the Trusted Root Recipients

For details, see [“Importing a Trust Anchor and Setting Trust” on page 14.](#)

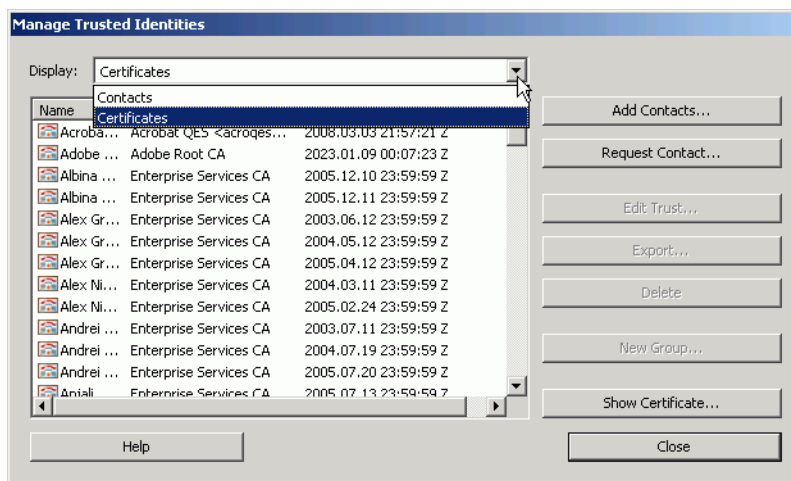
Optional: Setting Certificate Trust Level

Tip: This section is only relevant for trust anchor’s in FDF files that are signed with a trusted signature. This is an unlikely scenario, since the trust anchor distributor is probably using the same trust anchor that is being distributed and the recipient doesn’t have it yet. Most users will likely need to manually set the imported certificate’s trust level.

When distributing a trusted root in a signed file that the FDF recipient can validate, set the certificate trust level:

1. Choose **Advanced > Manage Trusted Identities.**
2. Choose **Certificates** in the **Display** drop down list.

Figure 22 Certificates in the Trusted Identities list



3. Highlight the needed certificate.
4. Choose **Edit Trust.**
5. Display the Trust tab.
6. Set the trust level as described in [“Importing a Trust Anchor and Setting Trust” on page 14.](#)

Exporting Your Certificate

You can use FDF files to export your certificate so that others can import it into their list of trusted identities. This enables them to encrypt documents for you and validate your signature for documents that you digitally sign.

- Before users receiving your signed document can validate your signature, they must receive the your certificate or one above it in the trust chain.
- Before users can encrypt a document for you with certificate encryption, they must have access your certificate.

Certificates can be emailed or saved to a file for later use. There are two ways to export a certificate:

- To export a certificate from the list in the Security Settings dialog, refer the following:
 - [“Emailing Your Certificate” on page 22](#)
 - [“Saving Your Digital ID Certificate to a File” on page 23](#)
- To export any certificate displayed in the Certificate Viewer, choose **Export** on the General tab.

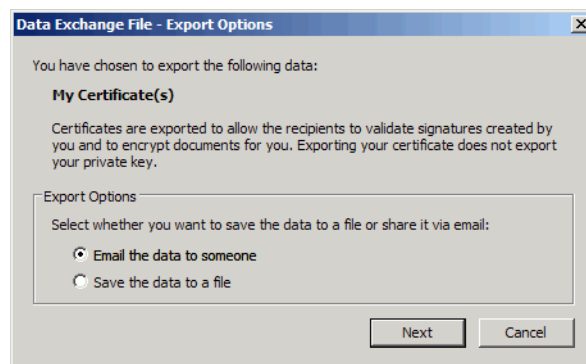
Emailing Your Certificate

If you do not have an email program on your machine (such as Outlook), save the data to a file as described in [“Saving Your Digital ID Certificate to a File” on page 23](#) and then send the file as an attachment using your web-based email program.

To email a digital ID certificate:

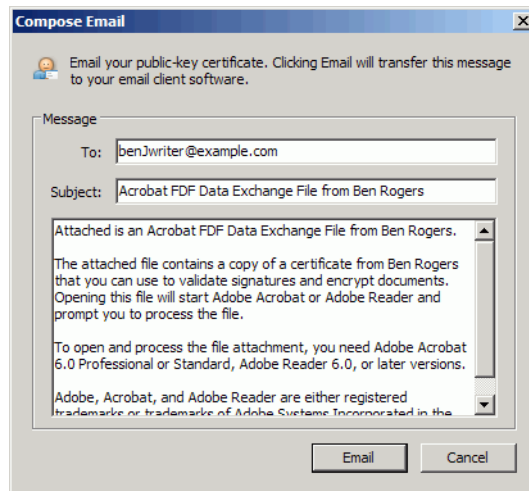
1. Choose **Advanced > Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Highlight an ID in the list on the right.
4. Choose **Export**.
5. Choose **Email the data to someone** ([Figure 23](#)).

Figure 23 Digital ID: ID export options



6. Choose **Next**.
7. Enter the recipient's email address and any other optional information.

Figure 24 Emailing a digital ID



8. Choose **Email**.
9. When the email program opens, send the email.

Saving Your Digital ID Certificate to a File

To save a digital ID certificate to a file:

1. Choose **Advanced > Security Settings**.
2. Select **Digital IDs** in the left-hand tree.
3. Highlight an ID in the list on the right.
4. Choose **Export**.
5. Choose **Save the exported data to a file** (Figure 23).
6. Choose a file type:
 - **Acrobat FDF Data Exchange**: FDF files enable the easy exchange of data between any Acrobat family of products.
 - **Certificate Message Syntax - PKCS#7**: Save the file as a PKCS7 file. Use this format when the data will be imported into a non-Adobe store such as the Macintosh key store or Windows Certificate Store.
7. Choose **Next**.
8. Browse to a file location and choose **Save**.
9. Choose **Next**.
10. Review the data to export and choose **Finish**.

Requesting a Certificate via Email

When you request digital ID information from someone, the application automatically attaches to the email an FDF file containing your contact information and certificate.

To request a certificate from someone:

1. Choose **Advanced > Manage Trusted Identities**.
2. Choose **Request Contact**.

Figure 25 Emailing a certificate request

Email a Request

Email a request for a copy of someone else's certificate. You may use the certificate to validate signatures from that person as well as encrypt documents for that person.

My Identity

My Name: Ben Writer

My Email Address: b_writer@example.com

The recipient of your request may use your contact information (e.g., phone number) to verify that you are the one who sent this request.

My Contact Information: Some Known Info

You can also send your certificates so the recipient can validate your signatures and encrypt documents for you.

Include my Certificates

Email request
 Save request as a file (do not email now)

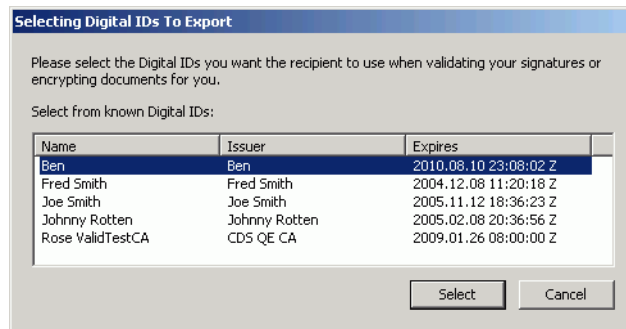
Next Cancel

3. Confirm or enter your identity so that the recipient can identify you.

Tip: The identity panel is prepopulated if the information has been previously configured in **Edit > Preferences > Identity**.

4. Choose **Include My Certificates** to allow other users to add your certificate to their list of trusted identities.
5. Choose whether to email the request or save it as a file.
6. Choose **Next**.
7. Select one or more digital IDs to export. Highlight contiguous IDs by holding down the Shift key. Highlight non-contiguous IDs by holding down the Control key.

Figure 26 Certificates: Selecting a digital ID for export



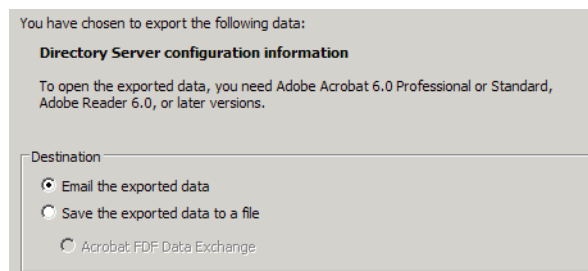
8. Choose **Select**.
9. The next step varies depending on whether you chose to email the ID:
 - **If you chose Email:** Enter the person's email address in the Compose Email dialog and choose **Email**. Send the email message when it appears in the launched email application with the certificate request attached.
 - **If you chose Save as file:** Choose a location for the certificate file Export Data As dialog. Choose **Save**, and then choose **OK**. Tell the intended recipient(s) where to find the file.

Emailing Server Details

Adobe Policy Server, directory server, roaming credential server, and timestamp server details can be exported to an FDF file for distribution to one or more people. Server information sent via an email resides in an attached FDF file. To send directory server details in an email:

1. Choose **Advanced > Security Settings**.
2. Select a server category from the left-hand list.
3. Select a server from the right-hand panel.
4. Choose **Export**.
5. Choose **Email the exported data** to email the FDF file.

Figure 27 Digital ID Directory servers: Export destination



6. Choose **Next**.

Tip: Configure the identity information if it is not already specified under **Edit > Preferences > Identity** (Figure 28). The Identity panel will not appear if the information has been previously configured.

Figure 28 Digital ID Directory servers: Sender's identify

Your identity information is used with comments, reviews, and digital signatures. Information entered here is secure and not transmitted beyond this application without your knowledge. To modify this information in the future, simply go to the Identity panel in the preferences.

Identity

Login Name: brogers

Name:

Title:

Organization Name:

Organization Unit:

Email Address:

Do not show again

7. Choose **Sign** and complete the signing workflow (Figure 10). Sign FDF files so that recipients of the file can easily trust the file and its contents.
8. Choose **Next**.
9. Enter the email information.

Figure 29 Digital ID Directory servers: Email details

You can specify the contents of the email message to which you will attach the exported data. This information will be sent to your email program.

Message

To:

Subject:

Attached is an Acrobat FDF Data Exchange File from Neb Whifflesnit.

The attached file contains search directory configuration information that can be used to access search identity directories.

Opening this file will start Adobe Acrobat or Adobe Reader and prompt you to process the file.

To open and process the file attachment, you need Adobe Acrobat 6.0 Professional or Standard, Adobe Reader 6.0, or later versions.

10. Choose **Next**.
11. Review the export details.
12. Choose **Finish**.

Exporting Server Details

Adobe Policy Server, directory server, roaming ID, and timestamp server details can be exported to an FDF file for distribution to one or more people. Server information can be written to a file and saved to any location.

To save server details to a file:

1. Choose **Advanced > Security Settings**.
2. Select a server category from the left-hand list.

Note: For roaming ID server settings, choose an account under **Roaming ID Accounts**.

3. Select a server from the right-hand panel.
4. Choose **Export**.
5. Choose **Save the exported data to a file** to save the data in an FDF file that can be shared ([Figure 27](#)).
6. Choose **Next**.

Tip: Configure the identity information if it is not already specified under **Edit > Preferences > Identity** ([Figure 28](#)). The Identity panel will not appear if the information has been previously configured.

7. Choose **Sign** and complete the signing workflow ([Figure 10](#)). Sign FDF files so that recipients of the file can easily trust the file and its contents.
8. Choose **Next**.
9. Browse to a location in which to save the file.
10. Choose a file name and choose **Save**.
11. Choose **Next**.
12. Review the export details.
13. Choose **Finish**.