FileNet Forms Manager

Pre-Installation Guide

Release 5.0.0

August 2005

FileNet Corporation
3565 Harbor Boulevard
Costa Mesa, California 92626
800.FILENET (345.3638)
Outside the U.S., call:
1.714.327.3400
www.filenet.com

Notices

Typographical Conventions

Where applicable, this document uses the conventions in the following table to distinguish elements of text.

Convention	Usage
UPPERCASE	Environment variables, status codes, utility names.
Bold	Paths and file names, program names, clickable user-interface elements (such as buttons), and selected terms such as command parameters or environment variables that require emphasis.
Italic	User-supplied variables and new terms introduced in text.
<*italic*>	User-supplied variables that replace everything between and including the angle bracket delimiters (< and >).
`Monospace`	Code samples, examples, display text, and error messages.

Table of Contents

Configuring the Application Server for I-Sign

The I-Sign signature service requires a server certificate because the user's name and password are encrypted. A certificate establishes a level of trust when sending sensitive data over the Internet by verifying the identity of the server for the client.

Server certificates are available from a number of sources. You can buy them from Microsoft or Verisign. For most purposes, a certificate issued by a server on the corporate intranet is sufficient.

If you do not already have a certificate server in your company, a Windows Certificate server can be set up to issue certificates. Windows 2000 includes the Microsoft Certificate Services. To enable a Windows server to issue certificates, you need to install the Certificate Services component. This is a standard component of the operating system, but it is not installed by default.

If your users will be signing forms using the I-Sign signature service, configure the application server as described in this document for I-Sign before you install your eForms applications.

Important notes:

- You must have IIS installed on the application server.
- You must have access to Microsoft Certificate Services.

To configure the Application Server for I-Sign

1. Create a New Certificate (Task 1 on page 5).
2. Create the Certificate Request (Task 2 on page 5).
3. Issue the Certificate (Task 3 on page 6).
4. Create the Certificate (.CER) File (Task 4 on page 6).
5. Install the Certificate (Task 5 on page 6).

Task 1: Create a New Certificate

1. Open the **Internet Services Manager** (**Start\Programs\Administrative Tools\Internet Services Manager**). The Internet Information Services window is displayed.
2. On the **Tree** tab, expand the nodes until you find the **Default Web Site** node. For eForms for Open Client, find the f**nOpenClient > secure** folder. Right-click the node and select **Properties**.
3. Select the **Directory Security** page tab.
4. Click the **Server Certificate** button. The Welcome to the Web Server Certificate Wizard is displayed. Click **Next**.
5. Select 'Create a new certificate.' Click **Next**.
6. Select 'Prepare the request now, but send it later.' Click **Next**.
7. In the 'Name' field, enter a name for the certificate. In the 'Bit length' field, select a bit length option. Click **Next**.
8. Enter values for the organization and organization unit respectively. Click **Next**.
9. In the 'Common name' field, enter the common name for your site. The common name is the hostname of the server. Click **Next**.
10. Enter values in the 'Country/Region', 'State/province', and 'City/locality' fields. Click **Next**.
11. Click **Browse** to navigate to the location where you want to store the certificate request file. In the 'File name' field, enter a name for the certificate request. This text file is the encryption of the certificate. Click **Save**. Click **Next**.
12. On the Request File Summary page, check the information that you entered for the certificate request. Click **Next**.
13. Click **Finish**. Click **OK** to close the Default Web Site Properties page.

Task 2: Create the Certificate Request

1. Using your browser, connect to Microsoft Certificate Services. Click **Next**.
2. For the request type, select 'Advanced Request.' Click **Next**.
3. Select 'Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.' Click **Next**.
4. Navigate to the text file generated in the *Create a new Certificate* step above and copy the contents. Return to the Microsoft Certificate Server browser window. In the 'Saved Request' field, paste the contents of the text file.
5. Click **Submit** to complete the request.

Task 3: Issue the Certificate

NOTE You must have administration permissions to issue the certificate.

1. Open the Certificate Authority application (**Start\Programs\Administrative Tools\Certificate Authority**). The Certificate Authority window is displayed.
2. On the Tree tab, expand the nodes until you find the folder called **Pending Requests**. Click the folder. The certificate request you made should appear in the work area on the right side of the window.
3. Click the Required ID that appears in your work area. Select **All Tasks** and then select **Issue**.
4. To ensure that the certificate was issued, on the **Tree** tab, find the **Issued Certificate** folder. The certificate appears in the folder.
5. Close the Certificate Authority application.

Task 4: Create the Certificate (.CER) File

1. Using your browser, connect to Microsoft Certificate Services.
2. In the Microsoft Certificate Server browser window, select ‘Check on Pending Certificate.’ Click **Next**.
3. From the **Pending** list, select the certificate request that was issued. Click **Next**.
4. Select ‘Base 64 Encoded.’ Then click the **Download CA Certificate** link.
5. Select an appropriate location in which to store the .CER file.

Task 5: Install the Certificate

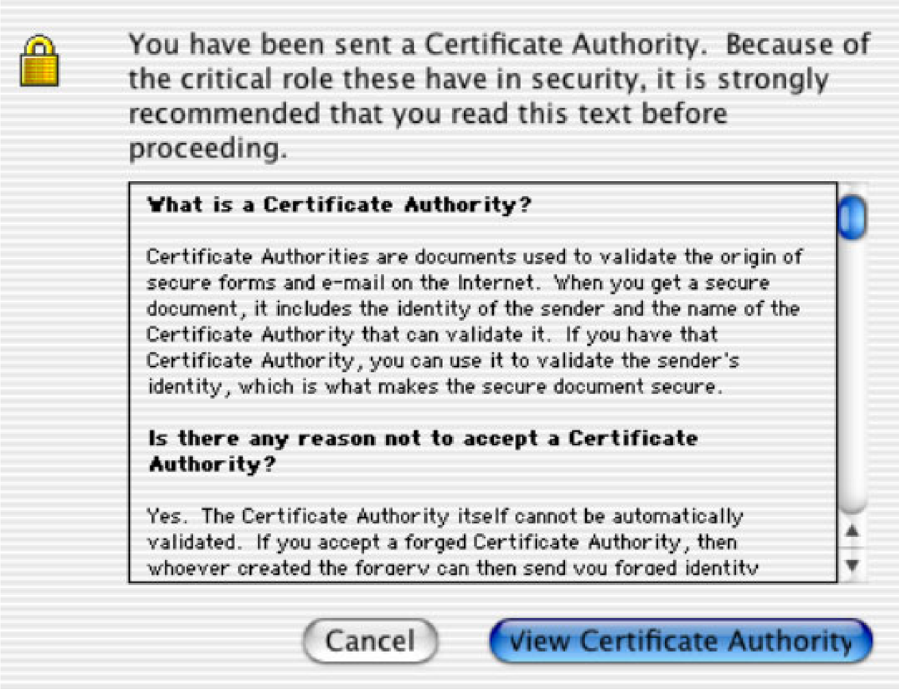
1. Open the Internet Services Manager (**Start\Programs\Administrative Tools\Internet Services Manager**). The Internet Information Services window is displayed.
2. On the **Tree** tab, expand the nodes until you find the **Default Web Site** node. Right-click the node and select **Properties**.
3. Select the **Directory Security** tab.
4. Click **Server Certificate**. The Welcome to the Web Server Certificate Wizard is displayed. Click **Next**.
5. Select ‘Process pending request and install the certificate.’ Click **Next**.
6. For the ‘Path and File name’ field, browse to the .CER file and select it. Click **Next**.
7. Check the summary information that appears. Click **Next**.
8. Depending on your server setting, a Certificate Enrollment window may appear. If this window appears, click **Yes**.
9. Click **Finish** to complete the installation of the certificate.

NOTE Before users sign forms, you must install the root certificate of the Certificate Authority (CA) into the user’s browser otherwise the user will receive an error message upon clicking the Sign button in the Signature dialog box (e.g., “Unable to establish a secure connection to [server name]. There is a problem with the security certificate from that site. The identity certificate issuer is unknown.”). For example, before a form is signed on Macintosh OS with Internet Explorer for Open Client, the issuer of the “trusted CA” certificate must be included with the internal list of “trusted CAs” for Macintosh Internet Explorer.

For Windows only instructions, see article “297681” in the Microsoft Knowledge Base at http://support.microsoft.com.

For Macintosh, follow these steps:

1. Browse to the website of the certificate issuer. You should be presented with a list of options. Select the option that allows you to retrieve the CA certificate or certificate revocation list.
2. Choose the certificate you want to download. Select the “Download CA certificate: DER Encoded” option.
3. The following window appears. Read the text and then click **View Certificate Authority**.



You have been sent a Certificate Authority. Because of the critical role these have in security, it is strongly recommended that you read this text before proceeding.

What is a Certificate Authority?

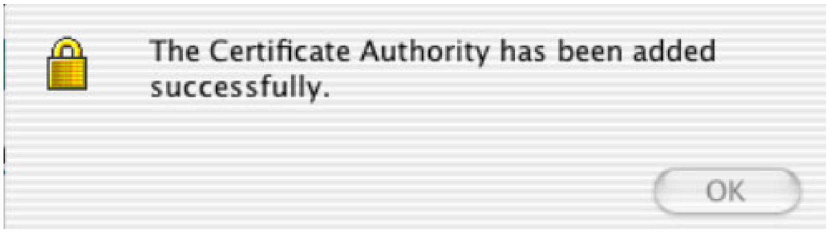
Certificate Authorities are documents used to validate the origin of secure forms and e-mail on the Internet. When you get a secure document, it includes the identity of the sender and the name of the Certificate Authority that can validate it. If you have that Certificate Authority, you can use it to validate the sender's identity, which is what makes the secure document secure.

Is there any reason not to accept a Certificate Authority?

Yes. The Certificate Authority itself cannot be automatically validated. If you accept a forged Certificate Authority, then whoever created the forgery can then send you forged identity

4. A Certificate Authority window appears. Select the options “I have verified that the Certificate is not a forgery” and “I trust the issuer to verify internet security”; then click **Accept**.
5. A password prompt window appears. As you create a password, ensure that you choose something that is easy to remember or record it somewhere. Click **OK** when finished. You must recall this password as you’ll be prompted later to enter it when connecting to the site for the first time during a session.

   With successful installation, the following confirmation message appears. Click **OK** to close the dialog box.



The Certificate Authority has been added successfully.

6. To view the certificate, choose **Explorer > Preferences**.
7. Click “Security” from the scrolling list. In the Certificate Authorities section, you can select the certificate and click **View**, **Change Password**, or **Delete**. Do not click **Reset to Defaults** unless you want to remove all non-default certificates.