

Entrust Entelligence™ Solo®

FAQ

Release 9.1
February 2010
Document issue: 1.0

Welcome to the Entrust Entelligence™ Solo 9.1 release.

This document answers some frequently asked questions about Entrust Entelligence Solo, referred to as 'Entrust Solo' throughout this FAQ.

- [What is Entrust Solo?](#)
- [How is Entrust Solo different from Entrust Entelligence Security Provider for Windows?](#)
- [What are the system requirements for Entrust Solo?](#)
- [How do I install Entrust Solo?](#)
- [Can I customize the software?](#)
- [How do I create a digital ID?](#)
- [How do I log in?](#)
- [How do I renew a digital ID?](#)
- [How do I back up a digital ID?](#)
- [How do I restore a digital ID from a backup copy?](#)
- [How do I change personal information in the digital ID, such as my name, or email address?](#)
- [What is the default key length, algorithm, expiry date, and CSP?](#)
- [How do I secure files?](#)
- [Can I use the command line to secure files?](#)
- [How do I access encrypted files \(.ent, .p7m, .pp7m, .exe\)?](#)
- [How do I secure email?](#)
- [How can I give others my encryption certificate so that they can encrypt for me?](#)
- [How do I check a signature on a file?](#)
- [Have another question?](#)

What is Entrust Solo? [\[top\]](#)

Entrust Solo is a small, desktop application that enhances the cryptographic functionality of the Windows operating system. Entrust Solo appears in the

Windows taskbar notification area (figure 1) and in a file's right-click menu (figure 2).



Figure 1: Entrust Solo in the taskbar

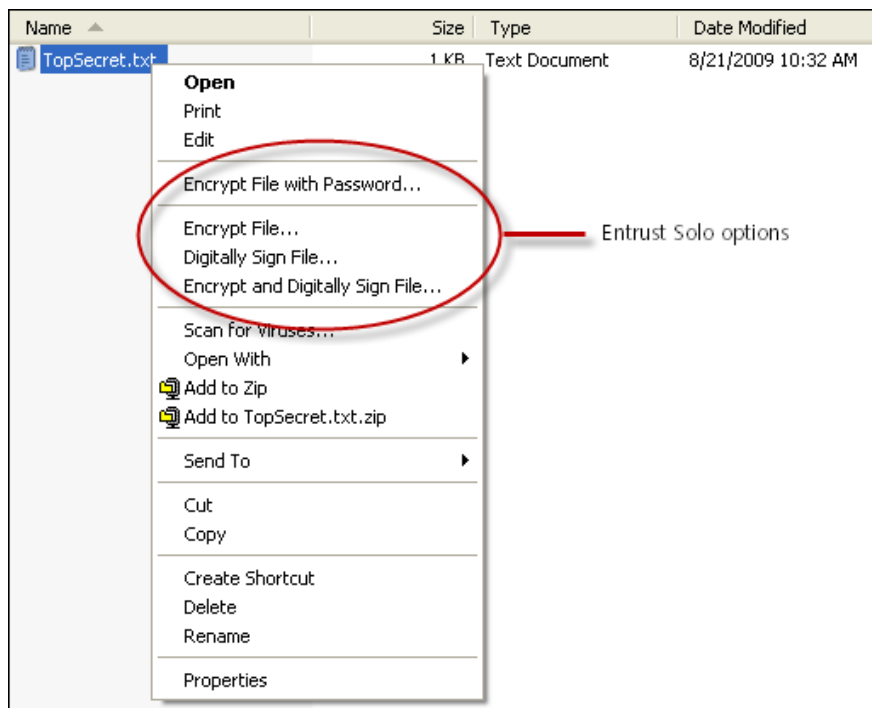


Figure 2: Entrust Solo in a file's menu

Specifically, Entrust Solo lets you:

- **create a digital ID**

A digital ID is an electronic document that is used to prove your identity, much like a driver's license or passport.

- **encrypt and digitally sign files with certificates**

When you encrypt a file with a certificate, only you and those you choose can access it. Digitally signing a file offers the same benefits as a handwritten signature.

- **encrypt files with a password**

You can encrypt a file with a password. The password will be asked for whenever anybody tries to open the file. You can keep this password to yourself, or distribute it to trusted people.

- **verify other people's digital signatures on files**

If someone else adds their digital signature to a file, you can verify the validity of this signature (expiry, name, and so on) using Entrust Solo.

- **decrypt files**

You can decrypt files that you have encrypted, or that have been encrypted for you by someone else.

- **get another person encrypting for you**

You can send your encryption certificate (that is in your digital ID) to another person so that they can begin encrypting files and email messages for you.

How is Entrust Solo different from Entrust Entelligence Security Provider for Windows? [\[top\]](#)

Entrust Entelligence Security Provider for Windows (or simply, 'Security Provider') offers similar functionality to Entrust Solo. These products differ in the following ways:

- Entrust Solo digital IDs are self-signed. Security Provider digital IDs are signed by a trusted third-party Certification Authority (CA).
- Entrust Solo digital IDs cannot be managed (revoked, disabled, and so on) by an administrator. Security Provider digital IDs can be fully managed.
- Entrust Solo does not communicate with a CA or other Public Key Infrastructure components. Security Provider communicates with a PKI, unless it is in off-line mode. Communication with a PKI is necessary in order to obtain the management features listed in the previous bullet.

- Entrust Solo does not include many of the enterprise features available with Security Provider such as TrueDelete, OCSP checking, and many more.
-

What are the system requirements for Entrust Solo? [\[top\]](#)

Entrust Solo is supported on Windows XP, Windows Vista, and Windows 7. For more detailed system requirements, see the *Entrust Solo Release Notes*.

How do I install Entrust Solo? [\[top\]](#)

Before installing Entrust Solo you must have purchased a license from Entrust. To purchase a license for Entrust Solo, contact an Entrust sales representative. To install Entrust Solo, follow the instructions below.

To install Entrust Solo

1. Ensure your computer meets or exceeds the system requirements. You need Windows XP, Windows Vista, or Windows 7. For more detailed requirements, see the *Entrust Solo Release Notes*.
2. Open a browser and navigate to the [Entrust TrustedCare Solo 9.1 download Web page](#). To access the site, use the user name and password provided to you in a customer letter.
3. Download `ESP_Solo_91_win32_install.zip` or `ESP_Solo_91_win64_install.zip` to your desktop depending on whether you are using a 32-bit or 64-bit processor.
4. Extract the ZIP file.
5. Open the extracted folder and double-click `eesolo32.msi` or `eesolo64.msi` to launch the installer.
6. On the Welcome page, click **Next**.
7. On the **End-User License Agreement** page, read the license, and if you agree to its terms, select the check box and click **Next**.
8. On the **Choose Setup Type** page, click **Typical** and click **Next**. (You can later [customize](#) your installation.)
9. On the **Install Entrust Intelligence Solo** page, click **Install**.
10. On the Completion page, click **Finish**.
11. On the dialog box asking you to restart your computer, click **Yes**. Your system is restarted.
12. Check that Entrust Solo was installed by clicking **Start > All Programs > Entrust Intelligence** and ensuring that Entrust Solo menu items appear.

Entrust Solo is now installed.

Can I customize Entrust Solo? [\[top\]](#)

Yes, you can customize Entrust Solo, but you don't have to. You can change settings related to which items are visible in the Entrust Solo menu.

To change Entrust Solo settings

Attention! The following procedure requires you to make changes to your Windows registry. If you are not familiar with the Windows registry, do not attempt this procedure. Configuration errors could cause your computer or Entrust Solo software to malfunction.

Note: If you are an administrator responsible for deploying Entrust Solo to multiple end-users, you can push out the registry settings described below to your user base in bulk using Windows Group Policy.

1. Unless the key is specified, you can add any of the entries listed below to your Windows registry under one of the following keys:

a) HKEY_CURRENT_USER > SOFTWARE > ENTRUST > ESP

b) HKEY_CURRENT_USER > SOFTWARE > POLICIES > ENTRUST > ESP

c) HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP

d) HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432Node > ENTRUST > ESP

e) HKEY_LOCAL_MACHINE > SOFTWARE > POLICIES > ENTRUST > ESP

f) HKEY_LOCAL_MACHINE > SOFTWARE > WOW6432Node > POLICIES > ENTRUST > ESP

Use **a)** if you want the settings to apply only to the currently-logged in user.

Use **b)** if you want the settings to apply only to the currently-logged in user and you are using Group Policy to push out the settings.


Use **c)** if you want the settings to apply to all users of the computer and you are using a 32-bit operating system.


Use **d)** if you want the settings to apply to all users of the computer and you are using a 64-bit operating system.

Use **e)** if you want the settings to apply to all users of the computer, and you are using Group Policy to push out the settings, and you are using a 32-bit operating system.

Use **f)** if you want the settings to apply to all users of the computer, and you are using Group Policy to push out the settings, and you are using a 64-bit operating system.

You can configure the following settings in the registry:

Setting	Details
SoloDigitalIDMonitorInterval	An interval (in hours) at which the digital ID is checked to see if it is near expiry. Type: DWORD Value: <number_of_hours> Default: 12 hours
SoloDigitalIDMonitorDaysToWarn	The number of days that a digital ID must be from expiring before renewal warnings begin appearing. Type: DWORD Value: <number_of_days> Default: 30 days
HideSoloCreateAppPersonalInTrayMenu	Determines whether to show the Create Entrust Solo Digital ID menu option when you right-click the  icon in the taskbar notification area. Type: DWORD Value: <1_or_0> 0 (default) = Show the Create Entrust Solo Digital ID menu option 1 = Hide the menu option
HideSoloManageAppInTrayMenu	Determines whether to show the Manage Entrust Solo Digital ID menu option when you right-click the  icon in the taskbar notification area. Type: DWORD Value: <1_or_0>

	<p>0 (default) = Show the Manage Entrust Solo Digital ID menu option</p> <p>1 = Hide the menu option</p>
HideSoloEmailAppInTrayMenu	<p>Determines whether to show the Email Entrust Solo Digital ID menu option when you right-click the  icon in the taskbar notification area.</p> <p>Type: DWORD Value: <1_or_0></p> <p>0 (default) = Show the Email Certificates menu option</p> <p>1 = Hide the menu option</p>
DigitalIDEmailMessage	<p>Use this setting to customize the email message used when you are exchanging certificates. Enter your customized message in a text file and enter the full path and the name of the file as the value. If Entrust Solo cannot find the file it will use the default message.</p> <p>Key: HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP Type: REG_SZ Value: <String> Default = default email message Where <String> is the complete path and filename of the text file.</p>
DigitalIDEmailAttachmentZipped	<p>Use this setting to specify that attached certificates should be zipped.</p> <p>When zipping certificates, a randomly generated password is created to protect the content. The user emailing certificates must provide the password to the other user. Also, the email message is changed to provide information about importing certificates.</p> <p>Key: HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP Type: REG_DWORD</p>

	<p>Value: <1_or_0> 0 (default) = Do not zip certificates 1 = Zip certificates and attach to email.</p>
DigitalIDEmailAttachCertificates	<p>Use this setting to attach certificates in .cer format. Key: HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP Type: REG_DWORD Value: <1_or_0> 0 (default) = Don't attach in .cer format 1 = Attach in .cer format</p>
DigitalIDEmailAttachP7CFile	<p>Use this setting to attach certificates as a .p7c file. Key: HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP Type: REG_DWORD Value: <1_or_0> 0 = Do not attach .p7c file 1 (default) = Attach .p7c file</p>
DigitalIDEmailNotification	<p>Use this setting to automatically send out replacement certificates if a new digital ID is created. Key: HKEY_LOCAL_MACHINE > SOFTWARE > ENTRUST > ESP Type: REG_DWORD Value: <1_or_0> 0 = Do not email certificates on digital ID creation or renewal. 1 (default) = Email certificates on digital ID creation or renewal.</p>

How do I create a digital ID? [\[top\]](#)

A digital ID is like a passport or driver's license: it provides proof of a person's identity. A digital ID contains cryptographic data including keys and certificates that let you encrypt information (files, for example) and apply digital signatures.

The following instructions describe how to create a digital ID and a back up copy should the original go missing.

Attention! Keep your digital ID in a safe place. If you lose it (and the backup), you will no longer be able to decrypt any files that you have encrypted for yourself using the certificate in the digital ID.

To create a digital ID

1. Right-click the Entrust Solo icon in the system tray (🌐) and select **Create Entrust Solo Digital ID**.
2. On the Welcome page, click **Next**.
3. On the **Information** page, do the following:
 - a. In the **Name** field, enter your first and last name, for example: Bob Smith
 - b. In the **Email** address field, enter your email address, for example bob.smith@company.com.
 - c. Click **Next**.
4. Review the confirmation page and click **Next**.
5. A **Security Warning** may appear, similar to the following:



Click **Yes** on the warning.

6. An **Entrust Security Store Location** page appears. An Entrust Security Store is a password-protected file that contains your digital ID. Select a folder in which to place this file and then click **Next**.
7. On the dialog box asking whether you want to create the Entrust security store, click **Yes**.
8. On the dialog box asking for an Entrust security store name, provide a name such as BobSmith and click **Next**.
9. On the **Entrust Security Store Password** dialog box, specify a password in the **Password** and **Confirm Password** fields and click **Finish**. You will need to enter this password any time you (or an application) requires access to the keys in the Entrust security store. Ensure that the password follows the rules and uses a combination of letters, numbers, and special characters (?, !, @, and so on).
10. On the **Backup** page, enter or browse to a folder location where a backup copy of your digital ID will be stored and click **Next**. A confirmation page appears, indicating that warnings may appear.

11. On the completion page, click **Finish**.

You have now created a digital ID.

How do I log in? [\[top\]](#)

This section describes how to log in when you see this dialog box:



To log in

1. In the **Name** field, ensure your Entrust security store is shown (see the figure, above). If it is not shown, click **Browse** and navigate to your security store. It has an .epf file extension and is by default located in `c:\Documents and Settings\\Application Data\Entrust Security Store\`.

Note: If the Application Data folder is missing, it is because Windows has hidden it from view. To make this folder visible, open Windows Explorer and click **Tools > Folder Options**. Under **Files and Folders > Hidden files and folders**, ensure that **Show hidden files and folders** is selected. Click **OK**. You can now see the Application Data folder.

The Entrust Security Store is where your digital ID is stored.


2. In the **Password** field, enter the password you specified when you initially created your digital ID.

How do I renew a digital ID? [\[top\]](#)

You must renew your digital ID if:

- it is approaching expiry
- you want to change your name in the digital ID
- you want to change your email address in the digital ID

To renew a digital ID

1. Right-click the Entrust Solo icon in the system tray () and select **Manage Entrust Solo Digital ID**.
2. On the Welcome page, click **Next**.
3. Select **Renew an existing Entrust Solo digital ID** and click **Next**.
4. On the **Entrust Solo Digital ID Selection** page, select the digital ID you want to renew from the top-most list. (There may only be one listed.) The digital ID's corresponding encryption and verification certificates appear underneath. You can view details on either of these certificates by selecting the certificate and clicking **View Certificate**. When you have finished, click **Next**.
5. If a log in dialog box appears, enter the password that you specified when you created your digital ID and click **OK**.


An **Information** page appears where you can specify a name and email address.

6. Follow steps 3 - 6 under [To create a digital ID](#) to renew your digital ID. Click **Finish** to complete the process.

How do I back up a digital ID? [\[top\]](#)

A backup copy of your digital ID is generated for you when you create your digital ID. If this backup becomes lost, corrupted, stolen, or otherwise inaccessible, you can make another backup using the instructions below.

To back up a digital ID


1. Right-click the Entrust Solo icon in the system tray () and select **Manage Entrust Solo digital ID**.
2. On the Welcome page, click **Next**.
3. Select **Back up an existing Entrust Solo digital ID** and click **Next**.
4. On the **Entrust Solo Digital ID Selection** page, select the digital ID you want to back up from the top-most list. (There may only be one listed.) The digital ID's corresponding encryption and verification certificates appear underneath. You can view details on either of these certificates by selecting the certificate and clicking **View Certificate**. When you have finished, click **Next**.
5. If a log in dialog box appears, enter the password that you specified when you created your digital ID and click **OK**.

How do I restore a digital ID from a backup copy? [\[top\]](#)

If your primary digital ID becomes lost or corrupted, you can revert to your backup copy. If you cannot remember where your backup copy is, you can simply create a new digital ID.

Attention! If you lose your digital ID, and cannot find the backup, you will no longer be able to decrypt any files that you have encrypted for yourself using the certificate in the digital ID.

To restore a digital ID from backup

1. Right-click the Entrust Solo icon in the system tray () and select **Manage Entrust Solo Digital ID**.
2. On the Welcome page, click **Next**.
3. Select **Restore an Entrust Solo Digital ID from a backup** and click **Next**.
4. On the **Backup/Recover Entrust Solo Digital ID** page, do the following:
 - a. In the **Entrust Security Store backup** field, enter the location and file name of the file where the digital ID was backed up. For example, specify `c:\Documents and Settings\bsmith\My Documents\bobsmith.epfbak`. By default the backup digital ID is stored in `c:\Documents and Settings\\My Documents` where `<user>` is the name of the user who was logged in to Windows when the backup was taken.
 - b. In the **Entrust Security Store location** field, enter the folder where you want the restored digital ID to go, for example, `c:\Documents and settings\bobsmith\Application Data\Entrust Security Store`.
 - c. Click **Next**.
5. If a log in dialog box appears, enter the password that you specified when you created your digital ID and click **OK**.

- A confirmation page appears, indicating successful digital ID restoration.
6. On the confirmation page, click **Finish**.

Your digital ID is now restored.

How do I change personal information in the digital ID, such as my name, or email address? [\[top\]](#)

You can change the following personal information in your digital ID:

- your name
- your email address

To change your name or email address, you must renew your digital ID. For more information, see [To renew a digital ID](#).

What is the default key length, algorithm, expiry date, and CSP? [\[top\]](#)

Your digital ID is comprised of certificates and keys, among other information. To generate the keys, Entrust Solo uses the Entrust Enhanced Cryptographic Service Provider (CSP) with the RSA 2048-bit algorithm, and sets the keys to expire three year from the date of creation. These settings cannot be modified.

How do I secure files? [\[top\]](#)

There are four ways to secure a file using Entrust Solo:

- **You can encrypt the file with your certificate (which is part of your digital ID) and the certificates of others.** A file that is encrypted with your certificate is inaccessible to anyone but you. To access the file, you must enter your Entrust Solo digital ID password. Similarly, a file that is encrypted with the certificates of others is inaccessible to anyone except the owners of those certificates. To access the file, users must enter their digital ID passwords (if required).
- **You can encrypt the file with a password of your choosing.** A file that is password-encrypted requires you to enter the file's password to access the file. You can share this password with others to give them access to the file—they do not require encryption software or certificates.
- **You can digitally sign the file.** A digital signature provides the same benefits as a handwritten signature in that the signer cannot deny having signed the file. (This is known as non-repudiation.) Additionally, a digital signature guarantees that the file has not been altered since it was signed. (This is known as file integrity.)
- **You can sign and encrypt the file using certificates.** A file that is digitally signed and encrypted is one that:
 - cannot be repudiated (the signer cannot deny having signed the file)
 - has integrity (the file is guaranteed not to have changed since it was signed)

- o can only be accessed by you and other people whose certificates you selected.

For instructions, see:

- [To encrypt files with certificates](#)
- [To encrypt files with a password \(and optionally your certificate\)](#)
- [To digitally sign files](#)
- [To digitally sign and encrypt files with certificates](#)

You can also [use the command line to secure files](#).

To encrypt files with certificates

1. Open Windows Explorer.
2. Select a file, or select multiple files using Shift+click.
3. Right-click the files and select **Encrypt File**. A wizard appears.
4. On the Welcome page of the wizard, click **Next**.
5. On the **Encryption Options** page, do the following:
 - a. In the **Your Encryption Certificate** field, ensure your encryption certificate is displayed. It should read <your_name>'s **Encryption Certificate**, for example Bob Smith's Encryption Certificate. Click **Choose** to select a different certificate if the one displayed is incorrect. If you do not have an encryption certificate, you can obtain one by [creating a digital ID](#).
 - b. In the **Encrypt Algorithm** field, select any algorithm from the drop-down list. The higher the number of bits, the stronger the algorithm. The default, 3DES, is acceptable.
 - c. Select **Encrypt the files for other people in addition to myself** if you want to specify other people that are allowed to access the file(s). Click **Next**.
6. If the **Additional Recipients** page appears, do the following:
 - a. Click **Add** to add a person for whom you want to encrypt the file(s).
 - b. Select the certificate of the person or group for whom you want to encrypt. If the people or groups do not appear in the list, ensure that **All** is selected from the **Show** drop-down list. If the people or groups still do not appear, it is because you do not have their certificates on your computer. You must [obtain and import their encryption certificates](#) to your computer in order for them to be displayed in the list.
 - c. Click **OK** on the **Select People** dialog box.
 - d. Click **Next** on the **Additional Recipients** dialog box.

Entrust Solo encrypts the file, and gives it a .p7m extension.

7. On the completion page, optionally select **Delete the original files on finish** to delete the unencrypted version of the file and keep only the encrypted .p7m version. When you have finished, click **Finish**.

Your file is now encrypted and has a .p7m file extension.

To encrypt files with a password (and optionally, your certificate)

1. In Windows Explorer, select a file or select multiple files using Shift+click.
2. Right-click the files and select **Encrypt File with Password**.

The **Password Encrypt Files** wizard appears.

3. On the Welcome page, click **Next**.
4. On the **Encryption Options** page, do the following:
 - a. In the **Password** and **Confirm Password** fields, enter a password of your choosing. Ensure that all the red 'X's become green check marks.
 - b. Record the password and keep it in a safe place.

Attention! If you forget your password, and the **Encrypt the files for my encryption certificate in addition to the password** check box is deselected, there is no way to recover the file. There are no work arounds. Therefore, it is extremely important to write down your password and keep it in a safe place for future reference.

- c. If it is available, set the **Encrypt the files for my encryption certificate in addition to the password** check box.
 - If you select the check box, then when you try to access your password-encrypted file, you are prompted to log in to your digital ID. Select the check box if you think you will be more likely to remember your digital ID password than the file's password.
 - If you deselect the check box, then when you try to access your password-encrypted file, you are prompted to enter the file's password.
 - Regardless of whether you select or deselect the check box, other people who try to access the file are prompted for the file's password.
 - d. If you selected the **Encrypt the files for my encryption certificate in addition to the password** check box, ensure that your encryption certificate is listed in the **Your Encryption Certificate** field. Your encryption certificate has your name on it; for example, Bob Smith's Encryption Certificate. Select **Choose** to select your encryption certificate.
 - e. Click **Next**.
5. On the **Packaging Options** page, do the following:

- a. In the field showing the location and name of the .pp7m file, accept the location, or click **Browse** to choose another location.
- b. Set the **Combine all files into single output file** check box.
 - If you select the check box, then all selected files are encrypted into a single .pp7m file, called Encrypted.pp7m by default.
 - If you deselect the check box, Entrust Solo generates a separate .pp7m file for each selected file. For example, if you have two files called TopSecret.doc and Private.txt, then two .pp7m files will be created, called TopSecret.doc.pp7m and Private.txt.pp7m, by default.

Note: The **Combine all files into single output file** check box is only available if multiple files were selected for password-encryption.

- c. Set the **Generate self-decrypting output file** check box.
 - Select the check box to create an .exe file instead of a .pp7m file. The benefit of the .exe file is that it can be shared with people who do not have encryption software on their computer. For example, you could send the .exe file to an external partner, and as long as this person has the file's password, they can decrypt the file; there are no software requirements. The main disadvantage of .exe files is that they most likely cannot be emailed, because they are typically blocked by companies' email gateways in order to prevent the spread of viruses. Even if the recipient successfully receives an .exe over email, this person should not open it, as it could have been tampered with in transit. To work around this problem, you can use a USB stick to transfer .exes from one computer to another, or create a .pp7m file (see the next bullet).
 - Deselect the check box to create a .pp7m file. The benefit of a .pp7m file is that it can be emailed and is smaller than an .exe file. Users must have Entrust Solo, Security Provider for Windows, or the password unprotect utility to access a .pp7m file.

Note: The **Generate self-decrypting output file** check box is only available if **Combine all files into single output file** is selected.

- d. Click **Next**.
6. On the completion page, do the following:

- a. Optionally select **Delete the original files on finish** to delete the plaintext version of the file and keep only the password-encrypted .pp7m version.
 - b. Optionally select **Send files via email** to open your default email application with the password-encrypted file attached.
7. When you have finished, click **Finish**.

Your file now has a .pp7m extension indicating that it is password-encrypted.

To digitally sign files

1. Open Windows Explorer.
2. Select a file, or select multiple files using Shift+click.
3. Right-click the files and select **Digitally Sign File**. A wizard appears.
4. On the Welcome page of the wizard, click **Next**.
5. On the **Digital Signature Options** page, do the following:
6. In the **Your Signing Certificate** field, ensure your signing certificate is displayed. It should read <your_name>'s **Verification Certificate**, for example Bob Smith's Verification Certificate. Click **Choose** to select a different certificate if the one displayed is incorrect. If you do not have a verification certificate, you can obtain one by [creating a digital ID](#).
7. In the **Hash Algorithm** field, select the algorithm that will be used to create the digital signature. The higher the number, the stronger the algorithm. The default, SHA1, is acceptable.
8. Click **Next**.

Entrust Solo digitally signs the file for you, and gives it a .p7m extension.

9. On the completion page, optionally select **Delete the original files on finish** to delete the unsigned version of the file and keep only the signed .p7m version. When you have finished, click **Finish**.

Your file is now digitally signed and has a .p7m file extension.

To digitally sign and encrypt files with certificates

1. Open Windows Explorer.
2. Select a file, or select multiple files using Shift+click.
3. Right-click the files and select **Encrypt and Digitally Sign File**. A wizard appears.
4. On the Welcome page of the wizard, click **Next**.
5. On the **Encryption and Digital Signature Options** page, do the following:
 - a. In the **Your Encryption Certificate** field, ensure your encryption certificate is displayed. It should read <your_name>'s **Encryption Certificate**, for example Bob Smith's Encryption Certificate. Click **Choose** to select a different certificate if the one displayed is

- incorrect. If you do not have an encryption certificate, you can obtain one by [creating a digital ID](#).
- b. In the **Encryption Algorithm** field, select any algorithm from the drop-down list. The higher the number of bits, the stronger the algorithm. The default, 3DES, is acceptable.
 - c. Select **Encrypt the files for other people in addition to myself** if you want to specify other people that are allowed to access the file(s).
 - d. In the **Your Signing Certificate** field, ensure your signing certificate is displayed. It should read <your_name>'s **Verification Certificate**, for example Bob Smith's Verification Certificate. Click **Choose** to select a different certificate if the one displayed is incorrect. If you do not have a verification certificate, you can obtain one by [creating a digital ID](#).
 - e. In the **Hash Algorithm** field, select the algorithm that will be used to create the digital signature. The higher the number, the stronger the algorithm. The default, SHA1, is acceptable.
 - f. Click **Next**.
6. If the **Additional Recipients** page appears, do the following:
- a. Click **Add** to add a person for whom you want to encrypt the file(s).
 - b. Select the certificate of the person or group for whom you want to encrypt. If the people or groups do not appear in the list, ensure that **All** is selected from the **Show** drop-down list. If the people or groups still do not appear, it is because you do not have their certificates on your computer. You must [obtain and import their encryption certificates](#) to your computer in order for them to be displayed in the list.
 - c. Click **OK** on the **Select People** dialog box.
 - d. Click **Next** on the **Additional Recipients** dialog box.

Entrust Solo encrypts and signs the file, and gives it a .p7m extension.

7. On the completion page, optionally select **Delete the original files on finish** to delete the unsecured version of the file and keep only the secured .p7m version. When you have finished, click **Finish**.

Your file is now secure and has a .p7m file extension.

Can I use the command line to secure files? [\[top\]](#)

Yes. Use:

- `eeencrypt.exe` to encrypt or sign files with one or more certificates

- `eedecrypt.exe` to decrypt or verify certificate-encrypted or digitally signed files
- `eepe.exe` to password-encrypt files
- `eepd.exe` to password-decrypt files

For help with command line options, enter the name of the executable at the command line (for example, `eepe.exe`) and press Enter.

How do I access encrypted files (.ent, .p7m, .pp7m, .exe)?

[\[top\]](#)

How to access an encrypted file is different depending on how the file was secured. See one of the following sections:

- [Accessing a certificate-encrypted file \(.ent, .p7m\)](#)
- [Accessing a password-encrypted file \(.pp7m, .exe\)](#)

To access a certificate-encrypted file (.ent, .p7m)

1. Ensure that you have one of the following software packages on your computer:
 - Entrust Solo
 - Entrust Entelligence Security Provider for Windows

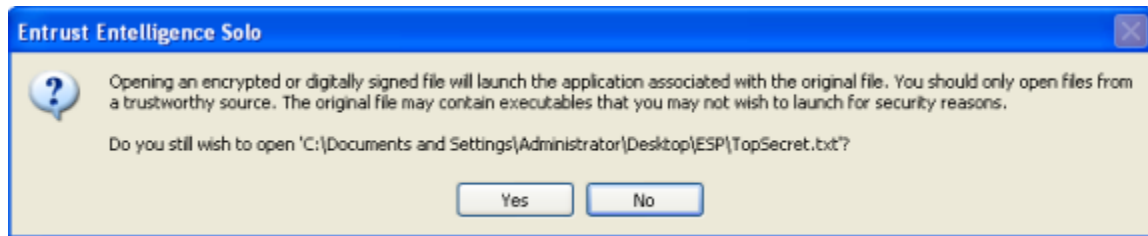
Without this software, it is impossible to access `.ent` and `.p7m` files.

2. Do one of the following:
 - a. If you want to access just one `.ent` or `.p7m` file, double-click it.
 - b. If you want to decrypt multiple `.ent` or `.p7m` files, shift-select them, then right-click the group, and then select **Decrypt and Verify**.

The **Entrust Security Store Login** dialog box appears.



3. Enter your security store password and click **OK**.
4. If the following dialog box appears, click **Yes** to open the file.



The file is decrypted, verified (if it was signed), and opened (if you selected to open it).

To access a password-encrypted file (.pp7m, .exe)

1. If you are trying to access a .pp7m file, ensure that you have one of the following software packages on your computer:
 - a. Entrust Solo
 - b. Entrust Intelligence Security Provider for Windows
 - c. Password unprotect utility (this utility is free, and is available from <http://www.entrust.com/passwordunprotect>)

Without one of these software packages, it is impossible to access .pp7m files.

Note: If you are trying to access a self-decrypting password-encrypted file (.exe), you do not require any special software.

2. Double-click the .pp7m or .exe file.
Either a password prompt or an Entrust Security Store Login dialog box appears.



3. Do one of the following:
 - a. If a password prompt appears, enter the file's password and click **OK**. If you do not know the password, ask the person who initially encrypted the file to give you the password.
 - b. If an **Entrust Security Store Login** dialog box appears, enter the password for your Entrust Solo digital ID and click **OK**.

The file is decrypted and placed in the same folder as the encrypted version. You can now open the decrypted file.



How do I secure email? [\[top\]](#)

You can exchange secure email with someone else. Consult one of the following procedures:

- [To exchange encrypted email](#)
- [To send a signed email message](#)



To exchange encrypted email

1. Ensure that you and the person you are emailing have email applications that support sign and encrypt functionality. Examples: Microsoft Outlook or Outlook Express.

2. Ensure that [you have installed the other person's encryption certificate](#), and [they have installed yours](#). Entrust Solo can be used to [create a digital ID](#).
3. Send encrypted email messages as follows:
 - If you are using Outlook, create an email message and click the encrypt button () in the toolbar. Alternatively, click **View > Options**. Click **Security Settings** near the top. Select **Encrypt message contents and attachments** and click **OK**. Close the **Message Options** dialog box. Send the message.
 - If you are using Outlook Express, create an email message and click the **Encrypt** button () in the toolbar. Send the message.
 - If you are using another email application, consult its documentation to encrypt the email.

Your message is encrypted and sent to the recipient.

To send a signed email message

1. Ensure that you and the person you are emailing have email applications that support sign and encrypt functionality. Examples: Microsoft Outlook or Outlook Express.
2. Ensure that you and the person you are emailing have digital IDs. You can use Entrust Solo to [create a digital ID](#).
3. Send signed email messages as follows:
 - If you are using Outlook, create an email message and click the sign button () in the toolbar. Alternatively, click **View > Options**. Click **Security Settings** near the top. Select **Add digital signature to this message** and click **OK**. Close the **Message Options** dialog box. Send the message.
 - If you are using Outlook Express, create an email message and click the **Sign** button () in the toolbar. Send the message.
 - If you are using another email application, consult its documentation to sign the email.

Your message is signed and sent to the recipient.

How can I give others my encryption certificate so that they can encrypt for me? [\[top\]](#)

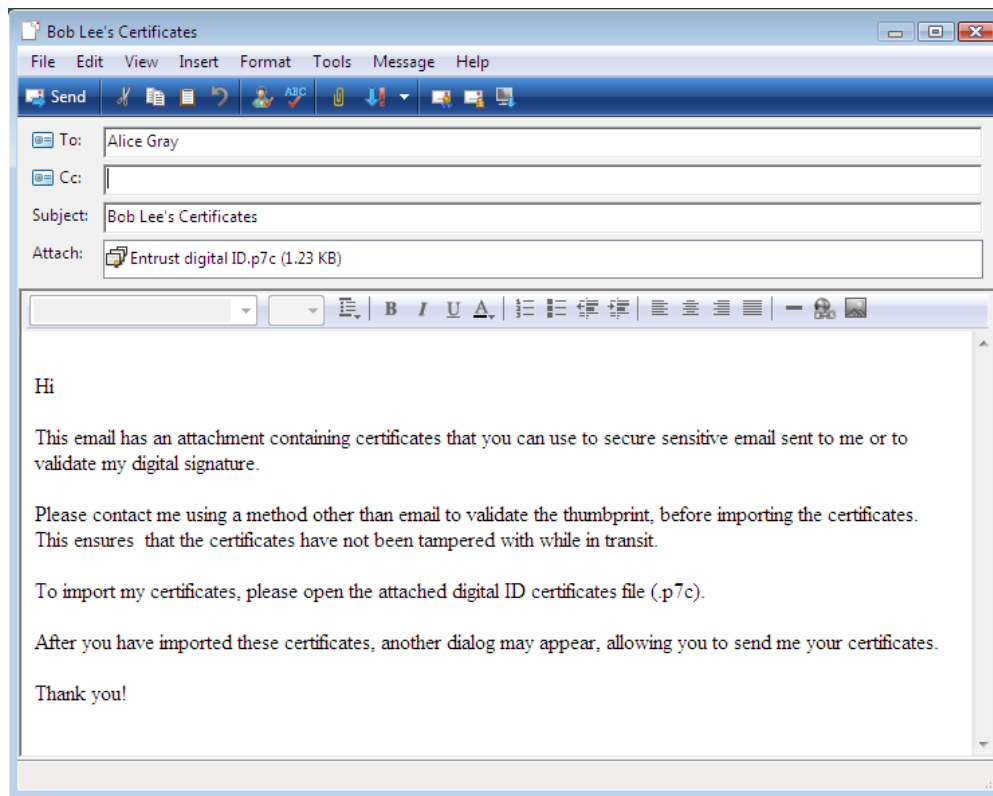
In order to encrypt information for you, other people need your encryption certificate which is part of your digital ID.

The following instructions describe how to send your encryption certificate to someone else, and how this person imports the certificate onto their computer.

To send your encryption certificate

1. Right-click the Entrust Solo icon in the system tray (🔒) and select **Email certificates**.
2. From the **Select a digital ID** list, select your digital ID. If no digital ID appears, [create a digital ID](#) for yourself. If multiple digital IDs appear, select yours, and check that it contains unexpired certificates. You can view details about a certificate by selecting it from the **Digital ID's certificates** list and clicking **View Certificate**.
3. Click **OK**.

Your email application opens with a pre-generated email. One or more certificates (in .p7c format, by default) are attached to the message.



4. Send the email to the people with whom you want to exchange encrypted email messages and files.

To import an encryption certificate


1. When someone receives an email from you that includes your certificates, have them follow the instructions in the email to import all of the

attached certificates. Once imported, the user can begin encrypting data for you using your encryption certificate.

How do I check a signature on a file? [\[top\]](#)

You may want to check a digital signature on a file to verify that it comes from the person you think it does, and also to ensure that its contents have not changed since the signature was applied.

To check a digital signature on a file

1. Right-click a file that has been secured and select **Properties**. Secured files are displayed with a lock icon (.
2. Click the Security Status tab. The signature information appears.
3. Verify the signature information. For example, ensure that the Signed By field contains the correct name.
4. Click Details.
5. Select **Signer:** <username> and click **Details**.
6. Click **View Certificate**.
7. Ensure that the **Valid to** date has not expired and that the other information seems correct.
8. Click **OK** to close the dialog.
9. Back in the **File Security Properties** dialog box, click the down-arrow next to **View Certificate** and select **View Timestamp Certificate** if the option is available.
10. Ensure that the timestamp date matches when you think the signature was applied.
11. Close all dialog boxes.

You have now checked a digital signature on a file.

Have another question? [\[top\]](#)

Contact your Entrust Solo sales representative.

© 2010 [Entrust](#). All rights reserved.

Published in Canada.

Entrust is a trademark or a registered trademark of Entrust, Inc. in certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust, Inc. in certain countries. All other company and product names and logos are trademarks or registered trademarks

of their respective owners in certain countries.

The information is subject to change as Entrust reserves the right to, without notice, make changes to its products as progress in engineering or manufacturing methods or circumstances may warrant.