

PKWARE[®]

Configure Outlook to Encrypt Messages when using SecureZIP Attachments for Windows

SecureZIP for Windows integrates with Microsoft Outlook to automatically secure all documents sent as message attachments to Email. Much of the information exchanged today using Email is sent as document files attached to messages. These documents are typically created, used and maintained outside of Outlook using other standard office applications such as Microsoft Word or Excel, and are then shared with others using the convenience of Email for exchanging information.

Increasingly, business documents and files must be protected from unauthorized access. The need for this protection often is in response to new audit or regulatory requirements that now mandate stronger data protection measures to safeguard data from malicious interception or loss. The need for these measures is understandable given that many of the files transferred may contain confidential personal, financial, or other high-value sensitive data, that if lost or intercepted, could place a company at serious risk of financial loss or litigation.

SecureZIP for Windows provides one-click protection of files transferred through Email. Every file you attach can be automatically compressed and encrypted when sent. SecureZIP protects the attached files during transfer through email as well as after the files are detached for use by their recipients. This presistent protection ensures data remains secure both in transit and at rest.

SecureZIP will protect all attached files, however, it does not provide encryption support for the message text (also called the message body) sent with attached files. While much of the high-value data is contained within the attached files that SecureZIP protects, sometimes confidential information may also be included within the message itself. You can combine SecureZIP encryption with Outlook's S/MIME message encryption feature to ensure both message content and attachments are protected. The following discussion illustrates how to configure SecureZIP to protect attached files and how to configure Outlook to protect their accompanying message.

PKWARE, the PKWARE Logo, and PKZIP are registered trademarks of PKWARE, Inc. SecureZIP is a trademark of PKWARE, Inc. Trademarks of other companies mentioned appear for identification purposes only and are the property of the respective companies.

Contents

Configure Outlook to Encrypt Messages when using SecureZIP Attachments for Windows			
Outlook Restrictions	3		
Configure SecureZIP for Windows to Secure Outlook Attached Files	4		
Point SecureZIP to Your Digital Certificates	5		
Configuring Local Encryption Certificates	5		
Locating Encryption Certificates in your Directory Service	5		
Specify a Default Certificate in SecureZIP	7		
Enable Email Security Features in SecureZIP	8		
Configuring Outlook for message encryption			

Outlook Restrictions

If you choose to encrypt your message content within Outlook, there are several restrictions you should make note of. These restrictions are not imposed when using only SecureZIP and they do not apply to your SecureZIP encrypted attachments. They apply only to the Outlook message encryption feature.

- To use Outlook's S/MIME encryption, you must obtain a digital ID. When using only SecureZIP encryption, you only need a digital ID if you choose certificate (or recipient-based) encryption. If you are already using certificates for encryption with SecureZIP, you can use your existing digital ID for encrypting Outlook messages. Steps for obtaining a digital ID are not covered in this guide and the discussion that follows assumes you have already obtained and installed your digital ID. If you need assistance on obtaining a digital ID, contact your System Administrator, your Security Administrator, or contact PKWARE Technical Support for additional information on where to get a digital ID. You can contact PKWARE Technical Support at http://www.pkware.com/business and developers/support/.
- Outlook message encryption does not support the use of a password or passphrase. You must exchange the public portion of your digital ID with each recipient before you can send any encrypted email messages to them. A digital ID consists of a digital certificate and a private key. Your digital certificate includes information about you and a public key. These make up the public portion of your digital ID that other people can use to encrypt data sent to you. Your private key remains protected in your possession and can be used only by you to decrypt data encrypted with your public key. When using SecureZIP, file attachments can be protected with a password or passphrase, a public key(s) or both, Outlook encryption will only work with public keys and does not support the option of password/passphrase encryption.
- While SecureZIP encrypted attachments can be protected with strong AES 256-bit encryption, Outlook messages cannot. You will only be able to use 3DES encryption for encrypting your message body. You can still separately configure SecureZIP to use stronger AES encryption to more strongly protect your attached files.

- While SecureZIP encrypted attachments can be transmitted efficiently using the standard ZIP compressed file format, Outlook encryption cannot compress your message. In fact, the S/MIME encryption used by Outlook may increase the size of your message.
- When encrypting messages using Outlook encryption, you must make certain that all recipients are using S/MIME capable email clients. Although, your SecureZIP attachments can be read using any ZIP-enabled Reader, encrypted message text must be opened using an S/MIME mail client.

Configure *SecureZIP for Windows* to Secure Outlook Attached Files

SecureZIP can be configured to secure your Outlook attached files. You can secure your attached files even if you choose not to encrypt your Outlook message. The steps for configuring SecureZIP can be initiated by choosing the SecureZIP icon located in your Windows desktop tool tray. Open the context menu and select **SecureZIP Options**.



To complete the steps for configuring SecureZIP to use digital certificates for encrypting and digitally signating your attached files, you must take the following actions:

• Point SecureZIP to the location of your digital certificates

- Specify a personal digital certificate to use by default for certificatebased encryption and digital signing
- Turn on encryption or signing in SecureZIP to have SecureZIP encrypt or sign files
- Enable email attachment features of SecureZIP

The sections that follow describe how to complete each operation.

Point SecureZIP to Your Digital Certificates

For SecureZIP to access the digital certificates of those people to which you will be sending encrypted attachments, you must tell SecureZIP where their certificates are stored. SecureZIP can locate certificates stored in two standard locations. The first location is your *local* Windows Certificate Store managed by your Windows Desktop operating system. Alternatively, SecureZIP can access certificates published using your enterprise LDAP-compliant directory service such as Active Directory. SecureZIP can be configured to look in both of these locations.

Configuring Local Encryption Certificates

SecureZIP will automatically locate certificates in your local Windows Certificate Store and no special configuration is required. However, before SecureZIP can find certificates in this store, they must be inserted using the Windows Certicate Import Wizard.

When you receive a certificate from someone to which you will be sending encrypted data, you will receive a .CER file. This file contains the digital certificate information and public key used when encrypting for that person.

To import a .CER file, select the file and open the Windows context menu. Choose the **Install Certificate** option to start the Windows Certificate Import Wizard. Follow the steps within the Wizard to import the certificate.

Locating Encryption Certificates in your Directory Service

To do this, open the tool tray context menu for SecureZIP and do the following. If you are not using a Directory Service, you can skip ahead to the next section.

- **1.** From the tool tray context menu, select **SecureZIP Options...** to open the SecureZIP Options dialog.
- **2.** Select the Security category.

3. Select the Certificate Stores tab to see a list of certificate stores SecureZIP can search.

The Certificate Stores list contains an item for every certificate store SecureZIP knows about. A store is labeled either *Local* or *LDAP* in the Type column, depending on whether the store is on your local system or on an LDAP-compliant directory server such as Active Directory. LDAP is a protocol used by Active Directory and other directory servers.

4. Choose the Add... button to open a new LDAP Properties page.

LDAP Properties		×
General		
Name:	PKWARE, Inc	
Server:	pkware.com	
Port:	389	
Protocol version:	3 🗸	
Base:	ou=pkware_inc,dc=pkware,dc=com	
Login:	Current logged-on account	
User:		
Password:		
ОК	Cancel Apply Help	

5. In the LDAP Properties dialog, fill in the fields with the information SecureZIP needs to access the directory. When done, choose **OK** to return to the Certificate Stores tab.

The fields in the LDAP Properties dialog are described in the following table. The fields marked *Optional* may be left blank unless they are required to access the server. Only the Name and Base fields are required by SecureZIP.

CONFIGURE OUTLOOK TO ENCRYPT MESSAGES WHEN USING SECUREZIP ATTACHMENTS FOR WINDOWS

Field	Description		
Name	A label to identify the server in the Certificate Stores list. For example: Gamma		
Server	(Optional) The IP address of the LDAP server or a name that resolves to such an address. For example: abc.company.com or 192.172.0.1		
Port	(Optional) The IP port to use. Port 389 is customary and is entered as the default.		
Base	The name of the entry that SecureZIP should use as the base or root of the LDAP search for certificates, analogous to a root folder or directory in a file system. For example: cn=users,dc=xyz,dc=com The guery string format for the LDAP base can vary between		
	LDAP implementations. For example, a server may expect query strings in the Internet domain-style format used by default by Microsoft Active Directory (for example, cn=users,dc=xyz,dc=com), or it may expect them in X.500 naming format (for example, o=xyz,c=US). Check with your LDAP or network administrator for the query string to use.		
Login	The login to use to access the LDAP server. Select one of the following:		
	Anonymous	Recommended where allowed by your Administrator, but not all LDAP servers allow anonymous access	
	Specified login	Use if no other choice is available. Passes the userid/password over the network in the clear (unencrypted).	
	Current logged-on account	Allows a Windows client to connect to Active Directory using current Windows credentials. Does not pass passwords over the network in the clear.	
User	(Optional) The user account with which to log in if the LDAP server requires a login		
Password	(Optional) The password associated with the user account		

6. On the Certificates Stores tab, choose **OK** or **Apply** to save the new certificate store for SecureZIP to use.

Specify a Default Certificate in SecureZIP

Users may have one or more personal certificates that they use to encrypt or digitally sign files. If a user has only one certificate, SecureZIP automatically uses that certificate. If a user has more than one, the user can tell SecureZIP

CONFIGURE OUTLOOK TO ENCRYPT MESSAGES WHEN USING SECUREZIP ATTACHMENTS FOR WINDOWS

which certificate to use by default. If you have only one digital certificate you can skip ahead to the next section.

To specify a default certificate to always include when encrypting (so that the user can decrypt files he or she encrypts):

- **1.** From the tool tray context menu, select **SecureZIP Options...** to open the SecureZIP Options dialog.
- **2.** Select the Security category.
- **3.** Select the Encryption tab.
- **4.** In the Method dropdown, select one of the two *Recipient list* options to enable the list of personal certificates.

In the list, a valid certificate displays with a green check mark; an invalid certificate shows a red "X".

5. Select a certificate to use by default.

If you have only one, it is used automatically.

6. Click OK or Apply

To specify a default certificate to use when signing:

- **1.** From the tool tray context menu, select **SecureZIP Options...** to open the SecureZIP Options dialog.
- **2.** Select the Security category.
- **3.** Select the Authentication tab.
- **4.** Select a certificate to use by default from the list of your personal certificates.

If you have only one certificate, it is used automatically. A valid certificate displays with a green check mark; an invalid certificate shows a red "X".

5. Click OK or Apply

Enable Email Security Features in SecureZIP

For SecureZIP to automatically secure attached files you must turn on the Email encryption and signing features of SecureZIP. SecureZIP then routinely encrypts and/or signs attached files until you turn these functions off.

CONFIGURE OUTLOOK TO ENCRYPT MESSAGES WHEN USING SECUREZIP ATTACHMENTS FOR WINDOWS

To do this, open the tool tray context menu for SecureZIP and do the following:

- **1.** From the tool tray context menu, select **SecureZIP Options...** to open the SecureZIP Options dialog.
- **2.** Select the Mail category.
- **3.** Check the box *ZIP attachments*.
- **4.** Check the box *Encrypt attachments*.
- If you want to digitally sign attached files, check the box *Sign Attachments*.
- If you want SecureZIP to automatically secure your attached files using public keys of the recipients designated in the **To:** field of your Outlook message, uncheck the box *Prompt before ZIPPING* and check the box *Auto-search for recipients*. This will instruct SecureZIP to automatically encrypt attachments for all recipients you've selected from your *Address Book*.

SecureZIP is now configured to secure all file attachments sent using Outlook. You can attach files to your messages using the **Insert File** feature within the Outlook message editor. Each file attached will be automaticlly protected by SecureZIP as soon as you press **Send** to send your message. SecureZIP will encrypt the files for each of the recipients you have selected to receive the message.

Configuring Outlook for message encryption

When protection is also required for the message text in addition to using SecureZIP to protect the attached files, you can configure Outlook to encrypt the message using the same digital ID used by SecureZIP.

To do this, open Outlook and do the following:

- **1.** From the menu bar, select **Tools** to open the Tools menu.
- 2. Select Options... to open the Options configuration dialog.
- **3.** Select the **Security** tab to display the security options.
- **4.** Check the box *Encrypt contents and attachments for outgoing messages*.
- If the list box labeled *Default Setting* is blank, you must also configure your security settings as follows:
- **1.** Choose the **Settings...** button to open the Change Security Settings dialog.

- **2.** Select the **Choose...** button adjacent to the Encryption Certificate field to open the Select Certificates dialog.
- **3.** Select the certificate you want to use for encryption and press **OK**.
- Outlook will automatically assume the same certificate will be used for digital signing. If you want to sign your messages with a different certificate, select the **Choose...** button adjacent to the Signing Certificate field and select your signing certificate from the Select Certificates dialog. Press **OK** to close the Select Certificates dialog.
- 4. Press OK to close the Change Security Settings dialog.
- 5. Press Apply on the Security tab to save your settings.
- **6.** Press **OK** to close the Options dialog.

Outlook is now configured to secure your message content as soon as you press **Send** to send your message. Only those designated recipients, as specified in the **To:** field, will be able to decrypt your message using their own private key. SecureZIP will continue to protect your attached files.