

# Configure *SecureZIP for Windows* for Entrust Entelligence™ Security Provider 7.x for Windows

SecureZIP for Windows interoperates with leading PKI vendors including Entrust, VeriSign, and RSA to enable the use of digital certificates for encryption and digital signing. This guide describes how SecureZIP interoperates with Entrust digital certificates and Entrust certificate stores. It assumes that you have already configured the Entrust Entelligence Security Provider 7.x for Windows and have generated end-user certificates.

For more information about installing and configuring the Entrust Entelligence Security Provider 7.x for Windows, please contact Entrust support:

<http://www.entrust.com/support/index.htm>

## Contents

<b>Configure <i>SecureZIP for Windows</i> for Entrust Entelligence™ Security Provider 7.x for Windows .....</b>	<b>1</b>
<i>Notes</i> .....	2
<i>Configure SecureZIP for Windows To Access Digital Certificates</i> .....	2
Point SecureZIP to Entrust Certificate Stores .....	2
Specify Default Certificates in SecureZIP .....	4
Turn On Encryption and/or Signing in SecureZIP .....	5
<i>Use Entrust Certificates for Encryption and Digital Signing</i> .....	6
Encryption Workflow .....	6
Decryption and Digital Signature Workflow .....	7

## Notes

- To access certificates stored in Entrust directories, SecureZIP requires the Directory Integration module, a separately licensed add-on to SecureZIP. SecureZIP integrates with LDAP-compliant directories, including Entrust, Microsoft Active Directory, Sun iPlanet, Novell eDirectory, and OpenSSL.
- SecureZIP co-exists with the Entrust Entelligence Desktop Manager on client machines. If you are using both SecureZIP and Entelligence Desktop Manager for different purposes, you may do so without interruption.

## Configure *SecureZIP for Windows* To Access Digital Certificates

To configure SecureZIP for Windows to use certificates for encryption and decryption and for working with digital signatures, you must take the following actions:

- Add the Entrust certificate store(s) to the list of stores SecureZIP checks for certificates
- For each end user, set a SecureZIP option to designate a personal certificate to use by default for certificate-based encryption and digital signing
- Turn on encryption or signing in SecureZIP to have SecureZIP encrypt or sign files

The following sections describe how to do each operation.

### ***Point SecureZIP to Entrust Certificate Stores***

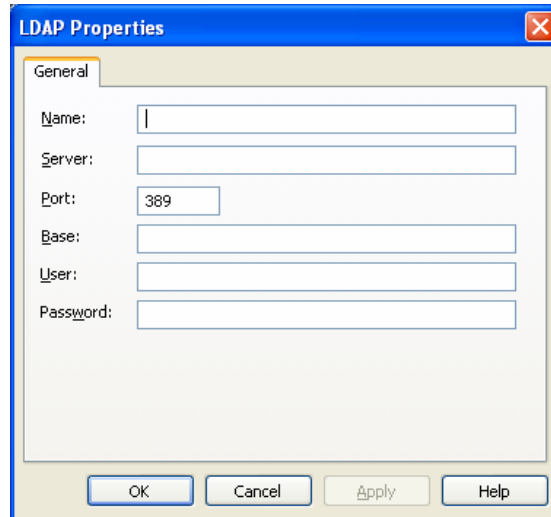
For SecureZIP for Windows to access Entrust certificates to encrypt for the certificates' owners, you must tell SecureZIP where the certificates are.

To do this, open SecureZIP and do the following:

1. In the Tools menu, select **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 an Entrust directory. LDAP is a protocol used by Entrust's directory and other directory servers.

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



5. In the LDAP Properties dialog, fill in the fields with the information SecureZIP needs to access the Entrust 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.

<b>Field</b>	<b>Description</b>
<b>Name</b>	A label to identify the server in the Certificate Stores list. For example: Gamma
<b>Server</b>	(Optional) The TCP/IP address of the LDAP server or a name that resolves to such an address. For example: 192.172.0.1
<b>Port</b>	(Optional) The TCP/IP port to use. Port 389 is customary and is entered as the default.
<b>Base</b>	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 query 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.
<b>User</b>	(Optional) The user account with which to log in if the LDAP server requires a login
<b>Password</b>	(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 Default Certificates 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 which certificate to use by default.

Because the certificates are different for each user, the following steps must be done for each user.

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

1. In SecureZIP, in the Tools menu, select **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. In SecureZIP, in the Tools menu, select **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**

### ***Turn On Encryption and/or Signing in SecureZIP***

To use certificates to encrypt or sign files in SecureZIP, those functions must be turned on. SecureZIP then routinely encrypts and/or signs files until you turn the functions off.

By default, encryption is turned on and signing is turned off.

To turn on certificate-based encryption:

1. On the Encryption tab of Security Options, in the Method dropdown list, select one of the following:
  - o Strong: Recipient List
  - o Strong: Recipient List or Password
2. Check the box *Encrypt files*.

See the SecureZIP help for other, more direct ways to turn on encryption.

To turn on signing, choose **Sign Files on/off** from the Actions menu. Again, there are other, more direct ways.

SecureZIP is now set up to do certificate-based encryption and apply digital signatures.

## Use Entrust Certificates for Encryption and Digital Signing

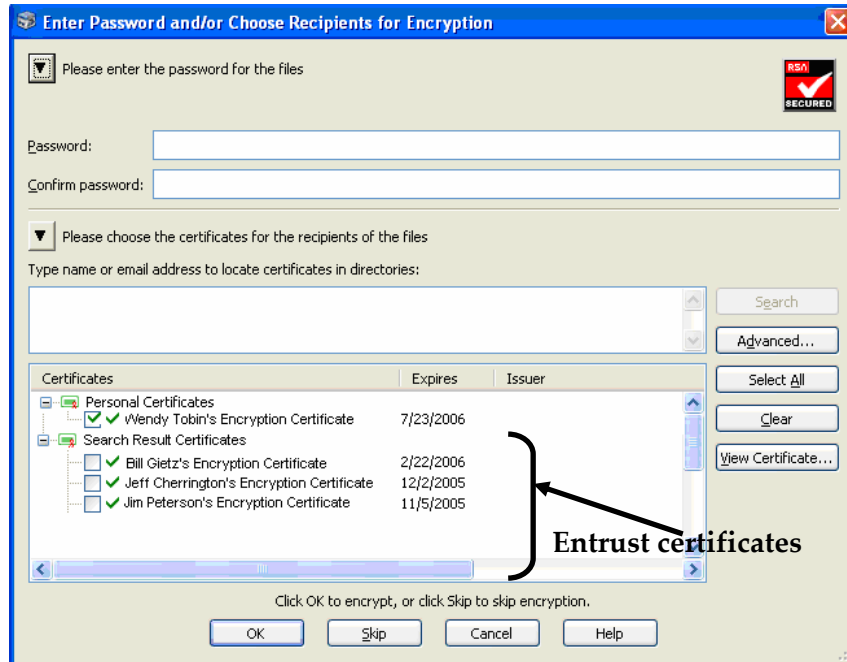
End users are now ready to begin using Entrust certificates to secure files with SecureZIP. Each end user has what Entrust refers to as a *security store*. The security store is where the end user's digital certificate resides. A certificate is comprised of a public and private key pair. The public key is used for encryption, and the private key is used for decryption and digitally signing files.

The following information describes how SecureZIP interacts with Entrust from an end user's perspective.

### ***Encryption Workflow***

During encryption end users are not required to be logged in to their Entrust security store. Rather, SecureZIP automatically locates the public key for encryption in the configured Entrust directory (Refer to the section above, "Point SecureZIP to Entrust Certificate Stores" for configuration details).

When encrypting, the SecureZIP user simply needs to select names of persons to encrypt for from the dialog shown below. The dialog displays when users encrypt files for a new or existing archive or for an email attachment sent using SecureZIP's Microsoft Outlook integration.



**Decryption and Digital Signature Workflow**

The end user must be logged in to the Entrust security store when decrypting or digitally signing files so that SecureZIP can access their private key. If the user is not logged in, but SecureZIP requires access to the private key, Entrust displays the login prompt shown below.



Once logged in, the end user can digitally sign files and/or decrypt files with SecureZIP.

**Note:** Entrust security stores can be configured to automatically log the user out after a set period of inactivity. A user who is logged out can simply log back in to continue using SecureZIP with certificates.