User’s Guide

SecretAgent 5
Register SecretAgent 5 now through our website, or by fax or mail. All we need is your name, address, phone number, serial number and date of purchase. You will be added to the list of registered SecretAgent licensees and be eligible to receive free technical support and product update notifications.

To Register On-line:


To Register By Fax:

♦ Fill out the registration form below and fax it to us at: (847) 405-0506.

To Register By Mail:

♦ Fill out the form below and mail it to us at:
  AT&T Security Software
  1141 Lake Cook Road, Suite D
  Deerfield, IL  60015-9461

Please add my name to your list of SecretAgent5 registered licensees.

____________________________________________________________
Company/Organization Name

____________________________________________________________
Name

____________________________________________________________
Address

____________________________________________________________
City                  State                  Zip

____________________________________________________________
Daytime Phone                        Purchase Date

Serial #
Technical support for *SecretAgent 5* is provided by Information Security Corporation as follows:

*For Technical Support*

Hours: 8:00 a.m. to 5:00 p.m. Central Time  
Voice: (847) 405-0757  
Fax: (847) 405-0506  
E-mail: tech@infoseccorp.com
Chapter 1: Introduction

Using this Guide ....................................................... 1-1
Conventions Used in this Guide ................................. 1-2
Printing Conventions ............................................. 1-2
Command Terminology ...................................... 1-3
Mouse Conventions ........................................... 1-3
Important Information .............................................. 1-4

Chapter 2: Installation

System Requirements ............................................... 2-1
System Software ................................................ 2-1
Hardware Requirements ..................................... 2-1
Installing SecretAgent 5 .......................................... 2-2
Running SecretAgent 5 for the First Time ................. 2-3
Certificates ........................................................ 2-3
User Personalities .............................................. 2-4

Chapter 3: Quick Start

Starting SecretAgent 5 .............................................. 3-2
SecretAgent 5 Views ................................................ 3-4
SecretAgent 5 Explorer .......................................... 3-4
Floating Toolbar View ........................................... 3-6
System Tray Menu .............................................. 3-7
Creating a New User Personality .............................. 3-8
Working with Certificates ...................................... 3-12
Working with Files ................................................. 3-16
Encrypting Files .............................................. 3-16
Decrypting Files .............................................. 3-18
Verifying Signed Files ..................................... 3-20
Signing Files ................................................... 3-22
Zapping Files .................................................. 3-23

Working with Office Suite Applications ................. 3-25
Encrypting a Document ................................... 3-25
Decrypting a Document ................................... 3-26

Exiting SecretAgent 5 ............................................. 3-27

Chapter 4: SecretAgent 5 Explorer

SecretAgent 5 Explorer Window .............................. 4-2
Tool/Menu Bar .................................................. 4-3
Go To Bar ....................................................... 4-10
All Folders and Contents Panels ...................... 4-11
Display Area Panel .......................................... 4-12

Working with SecretAgent 5 Explorer .................... 4-13
Encrypting Files .............................................. 4-13
Decrypting Files .............................................. 4-17
Signing Files ................................................... 4-20
Verifying Signatures ....................................... 4-21
Zapping Files .................................................. 4-23
Auto-Encryption and Auto-Decryption ............ 4-25

Chapter 5: Personality Manager

Personality Options and Preferences ..................... 5-1
General Tab ....................................................... 5-2
Encryption Tab .................................................. 5-3
Algorithms Tab .................................................. 5-6
Credentials Tab ................................................ 5-8
Output Tab ....................................................... 5-9
Plug-ins/Macros Tab ....................................... 5-12
Events Tab ...................................................... 5-13
Managing Multiple Personalities ....................... 5-15
Creating a New User Personality ....................... 5-15
Modifying a User Personality .......................... 5-19
Removing a User Personality ........................... 5-21

Chapter 6: Certificate Explorer
What is a Certificate? ............................................. 6-2
Secret Keys ...................................................... 6-2
Public and Private Keys .................................... 6-2
Certificate Explorer Window ............................... 6-3
Tool/Menu Bar .................................................. 6-4
Available Connections Panel .............................. 6-4
Contents Panel .................................................. 6-5
Creating Certificates .......................................... 6-6
Creating a Self-Signed Certificate .................... 6-6
Creating a Certificate Request ......................... 6-10
Importing, Exporting, and Sending Certificates ..... 6-15
Importing a Certificate .................................... 6-15
Exporting a Certificate ................................... 6-19
Sending a Certificate ..................................... 6-20
Deleting a Certificate ..................................... 6-22
Modifying Certificate Properties ..................... 6-23
New Certificate Wizard ...................................... 6-25
Entering Personal Information ......................... 6-25
Selecting a Key Type ...................................... 6-27
Validity Period and Key Usage Settings ............ 6-28
Specifying a Password ................................... 6-29
Storing the Certificate .................................... 6-30
Chapter 7: Application Integration

Integration with Third Party Applications................. 7-1

SecretAgent 5 and Microsoft Word .......................... 7-2
Encrypting a Word Document ............................... 7-2
Decrypting a Word Document ............................... 7-4

SecretAgent 5 and Microsoft Excel .......................... 7-5
Encrypting an Excel Spreadsheet............................ 7-5
Decrypting an Excel Spreadsheet............................ 7-7

SecretAgent 5 and Microsoft PowerPoint .................... 7-8
Encrypting a PowerPoint Presentation...................... 7-8
Decrypting a PowerPoint Presentation...................... 7-10
CHAPTER 1

Introduction

SecretAgent 5 uses the latest in encryption and digital signature technology to ensure the confidentiality, integrity, and authenticity of your data.

SecretAgent 5 for Windows is fully compatible with Windows 95, Windows 98, Windows NT 4.0 Workstation and Server operating systems, and Windows 2000. The program supports intuitive, user-friendly procedures such as drag-and-drop file operations and offers context menus to speed access to frequently used features.

Using this Guide

This User’s Guide provides information that will assist you in effectively using SecretAgent 5 for Windows. It is divided into seven chapters:

Chapter 1, Introduction
Provides an overview of the organization and contents of the guide, presents the style conventions used, and gives you an overview of how to install, configure, and use the features built in to SecretAgent 5.

Chapter 2, Installation
Provides the system software and hardware requirements and instructions for installing SecretAgent 5 on your computer and running SecretAgent 5 for the first time.
Chapter 3, Quick Start
Present the key steps needed to begin working with SecretAgent 5 and provides references to the procedures and detailed information contained in the other chapters.

Chapter 4, SecretAgent 5 Explorer
Describes the operation of SecretAgent 5 Explorer, showing how to use it to encrypt, decrypt, sign, verify, and zap files. Also described are SecretAgent 5’s automatic file encryption and decryption capabilities.

Chapter 5, Personality Manager
Describes the operation of the SecretAgent 5 Personality Manager, showing how to add a new user, change personality options and preferences, and modify a user’s personality.

Chapter 6, Certificate Explorer
Describes the operation of the SecretAgent 5 Certificate Explorer, showing how to create, modify, and delete a certificate.

Chapter 7, Application Integration
Shows how to access and use SecretAgent from within office productivity suites.

Conventions Used in this Guide
This User’s Guide consistently employs certain text formatting and language conventions to assist you in learning how to use SecretAgent 5.

Print Conventions
The following typographical conventions are used throughout this guide for screen displays, command entries, and keyboard characters:
Actions in procedures are printed in **bold type**.

Windows titles, menu names, and dialog names are printed exactly as they appear in the application.

Actions requiring key combinations are joined with a plus sign, *e.g.*, `<Ctrl + P>`. To execute this type of action, press and hold the first key, then press the second key and release both keys.

**Command Terminology**

The following terminology is used consistently in describing individual or multi-step actions.

- **Select** refers to making a choice from a menu or list of options in a dialog box. For example, “select the **Self-signed Certificate** option” means that you must select this option by clicking on it with the mouse.

- Steps that involve making two or more successive selections are often presented in combination. For example, when you read “Select **Personality, Preferences** from the Menu bar,” click **Personality** on the Menu bar and then select **Preferences** from its drop-down list.

**Mouse Conventions**

The assumption throughout this User’s Guide is that your left mouse button is configured as the Windows primary mouse button and that the right button is the secondary button. (You may, of course, choose to reverse the roles of these buttons using Windows’ Mouse Control Panel.) The following terminology regarding mouse usage is employed throughout this manual:

- **Click** means to position the mouse cursor over an object and then to press and immediately release the primary button without moving the mouse.

- **Double-click** means to position the mouse cursor and then to press and immediately release the primary button twice in quick succession.
Drag means to position the mouse cursor over an object (the source of the drag operation) and then to press and hold the primary button while moving the cursor to a new location. Once the cursor has reached its destination, release the mouse button to “drop” the object onto the target.

Important Information

Before installing or using SecretAgent 5 for the first time, please review the README.TXT file that may be included on the distribution media you received. This file may contain information that supersedes the information printed in this manual.

For technical support, call Information Security Corporation at (847) 405-0757 between 8:00 a.m. and 5:00 p.m. Central Time. You may also send email to tech@infoseccorp.com or fax your questions to (847) 405-0506.

Chapter 2

Installation

This chapter provides the basic information you’ll need to install and configure SecretAgent 5 on your computer:

- System Requirements
- Installing SecretAgent 5
- Running SecretAgent 5 for the First Time

System Requirements

System Software

SecretAgent 5 requires a 32-bit Microsoft Windows operating system: Windows 95, 98, NT 4.0 Workstation or Server, or Windows 2000. To use some of the user interface elements described below, you will also need to have Microsoft Internet Explorer 4.0 or higher installed on your system, though SecretAgent 5 will run without it.

Hardware Requirements

SecretAgent operates on any PC-compatible computer with an Intel Pentium-class processor or equivalent. The minimum hardware requirements are:

- 15MB of free hard disk space
- 16MB RAM
- VGA or better monitor
- Mouse and keyboard
- CD-ROM drive (unless you’re performing a network install)
Installing SecretAgent 5

The SecretAgent 5 installation process is automated. You must run the supplied Setup program to copy all required files to a specified directory on your hard drive and to ensure that all program components are properly registered with the operating system.

This section explains how to use the SecretAgent 5 Setup Program to load SecretAgent on to a stand-alone computer from the CD-ROM distribution media. (If you are installing from a network server, the SecretAgent 5 CD-ROM may not be required; consult your system administrator for instructions.)

To install SecretAgent 5:

1. Insert the SecretAgent 5 disc into your CD-ROM drive. If your drive supports Auto-Insert Notification and that feature is enabled in Windows, the SecretAgent Setup Program will start automatically. If this occurs, skip the next step and proceed to step 3; otherwise continue with step 2.

   Note: Please read all of the information in each dialog before advancing to the next step.

2. If the SecretAgent Setup Program does not start automatically, select Run from the Windows Start menu.

   Type D:\Setup in the Run dialog’s Open field and click OK to start the Setup Program. Be sure to substitute an appropriate drive letter if your CD-ROM drive is not D.
3. Follow the onscreen prompts provided by the installation wizard. After installation, you must restart your machine in order to use SecretAgent 5.

Running SecretAgent 5 for the First Time

When you use SecretAgent 5 for the first time, you will be prompted to set up a new personality (or user profile). This process usually involves the creation of a new certificate or certificate request, but you may also import an existing certificate for which you have the corresponding private key.

Certificates

A (public key) certificate is a “binding” of certain identifying information (typically a name, address, etc.) to one or more public keys. In creating a certificate, the issuing authority is, by applying its digital signature, affirming an association between the information and key(s) contained in the certificate.

SecretAgent 5 supports X.509 certificates issued by a trusted certificate authority (CA) to an individual as well as self-signed certificates (i.e., certificates issued by an individual on his own behalf to declare ownership of a particular public key and demonstrate possession of the associated private key).
The Certificate Wizard, built in to SecretAgent 5, guides you through the process of generating a self-signed certificate or a certificate request. See Chapter 6 Certificate Explorer for more information about the Certificate Wizard and procedures for generating, importing, exporting, and sending certificates.

User Personalities

SecretAgent 5 defines a personality (or user profile) to be a collection of user-specified preference settings together with a certificate (either self-signed or issued by a certificate authority). When a particular personality is active, its certificate (and associated private key) is used for all signing and decrypting operations. The active personality’s preference settings affect both the way the user interacts with SecretAgent 5 and the way the program works with the user’s files.

Only one personality may be active at any given time, but you may certainly create multiple personalities and switch between them freely.

The New Profile Wizard in SecretAgent 5 guides you through the process of adding a user personality. See Chapter 5 Personality Manager for information about the New Profile Wizard and user personality options, and procedures for creating and modifying a user personality.
CHAPTER 3

Quick Start

This chapter provides the basic information you need to work with SecretAgent 5. It is intended for first-time users of the product and provides a quick overview of some basic procedures. Users familiar with previous versions of SecretAgent may want to proceed directly to later chapters for more detailed information.

The procedures in this chapter assume you have completed the installation of SecretAgent 5 (see Chapter 2 Installation). First we explain how to start SecretAgent and present a brief overview of the three user interface views. Next we outline the process by which you create your first user personality (see Chapter 5 Personality Manager for more details) and associate with it a self-signed certificate (see Chapter 6 Certificate Explorer). Finally we outline the procedures used to apply the basic cryptographic operations to your files.

This chapter covers:

- Starting SecretAgent 5
- SecretAgent 5 Views
- Creating a New User Personality
- Working with User Certificates
- Working with Files
- Working with Office Suite Applications
- Exiting SecretAgent 5
Starting SecretAgent 5

When you install SecretAgent 5, a program group is created in your Windows Start Menu. The following procedure describes how to access SecretAgent 5 from the Start Menu.

To start SecretAgent 5:

1. Click the Windows Start button to display the Start menu:

2. Select Programs, SecretAgent 5, SecretAgent 5 to start the program. If you have only one personality defined, the SecretAgent 5 view you last used with that personality will open automatically; otherwise you will see the Personality Manager dialog box:
If the Personality Manager appears, select the personality you want to use and click **Login** to open the default SecretAgent 5 view for that personality. (You may also click **New** to create a new personality.) If there is only one defined personality, that personality will be automatically logged in and you will not see the Personality Manager dialog box.

Note: If this is your first time using SecretAgent, no personalities will appear in the Personality Manager dialog box and you'll need to create a new one. General information about working with personalities is presented later in this chapter. Detailed information about creating personalities may be found in Chapter 5 *Personality Manager* and Chapter 6 *Certificate Explorer.*
SecretAgent 5 Views

This section describes the three user interface configuration options, or views, available in SecretAgent 5:

- Explorer View
- Floating Toolbar View
- System Tray Menu

Choose the view that best matches the way you work. Whenever you start using a particular personality SecretAgent will automatically open the view you used last with that personality.

SecretAgent 5 Explorer

Explorer view is a compound window that is similar in appearance and function to Windows Explorer. This view consists of a function toolbar with drop-down menus and two panes (“All Folders” and “Contents”) above a tabbed display area (which may be hidden when not needed by clicking the blue arrow in the bottom left corner).
The buttons and drop-down menus on the toolbar provide access to all program features. The All Folders and Contents panes allow you to easily navigate through your file system in order to select the objects (files and/or folders) to be encrypted, decrypted, signed, validated or zapped.

Select the objects on which you want to operate in either of the upper two panes then choose the desired operation by clicking a button or choosing a menu item on the toolbar. For immediate action, you may also drag and drop objects directly onto the toolbar buttons from either upper pane or from another application.

We recommend Explorer view when your work involves using SecretAgent 5 as the primary application or when you need to perform a function that is not supported in the simpler views described below. You may use the drop-down menu next to the View icon to select one of the alternate views.

Chapter 4 SecretAgent 5 Explorer contains detailed information on this view.
Floating Toolbar View

Toolbar view contains only the button and drop-down menu area of the SecretAgent 5 Explorer window:

The Toolbar floats on the Windows desktop and may be dragged to any location providing instant access to all SecretAgent functions. You may use the buttons or menu items to select files on which to act. The buttons also accept files and/or folders dropped on to them from most other Windows applications, including Windows Explorer and the Windows Desktop.

Use this view when you are working in another application and only occasionally need quick access to common SecretAgent 5 functions. Just move the toolbar to a convenient location on your screen while your work in the primary application. The toolbar will then be available whenever you need to perform a cryptographic operation.

Note that the drop-down menu next to the view icon contains items you can use to switch to one of the other views.
System Tray Menu

In the System Tray view, a small SecretAgent 5 icon appears in the Windows System Tray (the right- or bottom-most pane of your Windows status bar). Click on this icon to display the SecretAgent 5 menu tree:

![System Tray Menu Diagram]

Items in the Files menu allow you to select one or more files to encrypt, decrypt, sign, verify, or zap. The Automatic Encryption submenu allows you to invoke the **AutoEncrypt Now** and **AutoDecrypt Now** commands. Clipboard... opens the clipboard viewer. You can also start Certificate Explorer or review and change the properties of your certificate by selecting your current personality. The Explorer and Toolbar items cause a switch to one of those alternate views. You can access online support using the three items in the next menu section, or exit SecretAgent entirely by selecting the final item.
Creating a New User Personality

A personality contains user-specified preferences and program settings that affect the way you interact with SecretAgent and the way SecretAgent works with your files. A particular personality (and its associated certificate) is in effect whenever SecretAgent is running. (More detailed information about working with personalities is included in Chapter 5 Personality Manager.)

The following procedure explains how to create a new user personality with the SecretAgent 5 default settings. The procedure assumes you are working within the SecretAgent 5 Explorer view. Based on the installation settings provided by your administrator, one or more of these options may not appear. Some options may appear, but be grayed out. These options cannot be changed.

To create a new personality:

1. Select Manage from the Personality menu to display the SecretAgent 5 Personality Manager:
2. Click **New** to start the New Personality Wizard.

3. Type a name for this personality in the Personality Name text box and click **Next**.

4. Select an appropriate credentials type from the list of available types. (The available choices will depend upon the various software and hardware token support modules that you installed with SecretAgent.)

5. Click **Next** to display the Select Certificate dialog box.
Note: You must have at least one certificate in your Personal Certificate folder. If you do not have a certificate, the SecretAgent 5 Personality Manager dialog box will allow you to create a certificate. To do this, click Yes when prompted to start Certificate Explorer (see Chapter 5).

6. Select the certificate to associate with the new personality name from the displayed list. (Note that as you highlight a particular Common Name, a more detailed description of that certificate will appear in the Certificate Information area.) Click on the desired certificate to make sure it is selected.

7. Click OK to accept the highlighted certificate and to display the New Personality Wizard’s Set default file locations dialog box.
8. Specify the names of the default folders in which you want to store the ciphertext and plaintext documents. Type in new folder names or click Select... to navigate through your folders to choose one.

9. Click Next to accept your folder settings. The New Personality Wizard’s Finished! dialog box will appear.

10. Click Finish to display the SecretAgent 5 Personality Manager dialog box. Your new personality will appear in the Available SecretAgent 5 Personalities area.
Working with Certificates

SecretAgent 5 requires you to possess a public key “certificate” that contains binds your identity to a specific public key. Certificates may be self-signed or issued by an authorized certificate authority (“CA”). Certificates allow correspondents to encrypt messages secure in the knowledge that only specified recipients can decrypt them. Certificates also allow receivers of a signed file to validate the signature and verify the identity of the signer. See Chapter 6 Certificate Explorer for more information about creating, or obtaining, a certificate, managing your private keys, and using SecretAgent 5 Certificate Explorer to access and maintain certificate databases.

The following procedure assumes you are working in the SecretAgent 5 Explorer window. It provides the principal steps for creating a new self-signed certificate using the default options. (If, on the other hand, your administrator has provided you with a certificate, or instructed you to generate a certificate request, you do not need to create a self-signed certificate. Instead, you will need to import the certificate returned by your CA. Please refer to Chapter 6 for instructions on this process.)

› To create a self-signed certificate:

1. Click the Certificates icon to display the Certificate Explorer.
2. Click **New** located above the available certificate panel to launch the New Certificate Wizard.

3. Select the **Self-signed certificate** option.

4. Click **Next** to display the Personal Information dialog box.

5. Type your personal information. Use the **Tab** key to advance to the next text box.

**Note:** If you are part of a group or network installation, your name and organization information will display automatically.
6. Click **Next** to display the Select Algorithms dialog box. Select the type of key and message digest to be generated for the algorithm used on this certificate.

7. Click **Next** to display the Set Validity Period and Extensions dialog box. The default usage allows you to encrypt and sign with a single certificate.

8. Click **Next** to accept the default settings and to display the Password dialog box.

9. Type your password in the upper text box. Retype your password in the lower text box for confirmation.
Note: Click **Suggest Password** to display the Generate Pronounceable Password dialog box to display a recommended character string that you could use as a password.

10. Click **Next** to display the Specify Disposition for Certificate/ Request dialog box.

11. Select the **Store the certificate or request in the active certificate folder** option. Click **Next** to display the Finished! dialog box.
12. Click **Finish** to close the Certificate Wizard and return to the Certificate Explorer window.

**Working with Files**

The most common operations performed with SecretAgent 5 are encrypting, decrypting, signing, verifying, and zapping files. A general procedure for each of these operations follows. The procedures assume that you are working in the SecretAgent Explorer view.

**Encrypting Files**

When you encrypt, first select one or more files, then specify whether to encrypt as a single output file, as separate output files, or as an archive.

The following procedure is for encrypting one file as a single output file from the SecretAgent 5 Explorer window. Other encrypting options are detailed in Chapter 4 *SecretAgent 5 Explorer.*
To select and encrypt a file:

1. Select **Encrypt, Encrypt...** on the Tool/Menu bar to display the Select Files to Encrypt dialog box.

2. Navigate through the folders and files. Click on the desired file to place its name in the File name text box.

3. Click **Open** to display the Encryption dialog box.

4. Select the **Separate files** Archive Type. A dot indicates an item is selected.

5. Select a recipient from the Available Certificates panel and click the **>>** button to place it in the Selected Recipients panel. You must pick yourself as a Selected Recipient to be able to decrypt the archive.

6. Click **OK** to begin the encryption process and display the Encrypt Progress dialog box.
7. Click **Close Window** to display the SecretAgent 5 Explorer window.

---

**Note:** The File Name and Encrypt status display in the Encrypt Progress panel and in the Event Log of the SecretAgent Explorer Display Area panel.

### Decrypting Files

The following procedure provides instructions for decrypting previously encrypted files from the SecretAgent 5 Explorer window. Other methods for selecting and decrypting files are covered in Chapter 4 *SecretAgent 5 Explorer*.

TextWriter

组 To select and decrypt a file from SecretAgent 5 Explorer:

1. Select **Decrypt, Decrypt...** on the Tool/Menu bar to display the Select Files to Decrypt dialog box.

2. Navigate through the folders and files and click on the desired file to place its name in the File name text box.
3. Click **Open** to display the Enter Password dialog box.

4. Type your password in the Password text box.

5. Click **OK** to begin the decryption process and display the Decrypt Progress dialog box.

![Decrypt Progress dialog box](image)

Note: The file name, decryption status, and plaintext file name display in the Decrypt Progress panels and in the Event Log of the SecretAgent Explorer Display Area panel.
6. (Optional) Select the Plaintext File and click **Open File** to launch the application in which the file was created and open the file.

7. Click **Close Window** to display the SecretAgent 5 Explorer window.

**Verifying Signed Files**

Verifying a file means that the digital signature associated with the file is checked to establish the authenticity of the sender and to ensure the recipient that the file has not been modified.

⇒ **To select a file and validate a signature:**

1. Click the **Verify** icon on the Tool/Menu bar to display the Select Files To Validate Signature dialog box.

![Select Files To Validate Signature](image)

2. Navigate through the folders and files. Click on the desired file to place its name in the File name text box.

3. Click **Open** to start the verifying signature process and display the Verify Progress dialog box.
Note: The file name, verification status, and plaintext file name display in the Verify Progress panel and in the Event Log of the SecretAgent Explorer Display Area panel.

4. (Optional) Select the File Name and click View Signature to display the Signature dialog box and see information about the signer.

5. Click Close or Close Window to display the SecretAgent 5 Explorer window.
Signing Files

Signing a file means that a digital signature is added to a file to ensure the recipient of the authenticity of the sender and that the file has not been modified.

To select a file and sign a file:

1. Click the **Sign** icon on the Tool/Menu bar to display the Select Files To Sign dialog box.

2. Navigate through the folders and files. Click on the desired file to place its name in the File name text box.

3. Click **Open** to display the Enter Password dialog box.

4. Type the user password in the Password text box.

5. Click **OK** to begin the signing process and display the Sign Progress dialog box.

Note: The file name and sign status display in the Sign Progress panel and in the Event Log of the SecretAgent Explorer Display Area panel.
6. Click **Close Window** to display the SecretAgent 5 Explorer window.

You may also instruct SecretAgent 5 to always add a signature to plaintext or e-mail by setting that option in your user personality. See Chapter 5 *Personality Manager* for additional information.

**Zapping Files**

Zapping a file deletes it permanently and it can not be recovered or undeleted. The zap option completely removes the source or plaintext file after it is encrypted so only the encrypted version remains on the disk.

**WARNING!**

Zapping a file permanently destroys the file. There is no way to recover a zapped file.

The following procedure explains how to zap a file from the SecretAgent 5 Explorer window.

⇨ **To zap a file from SecretAgent 5 Explorer:**

1. Click **Zap** on the Tool/Menu bar to display the Select Files to Zap dialog box.

2. Navigate through the files and click on the desired file(s).
3. Click **Open** to display the Confirm File Zap dialog box.

![Confirm File Zap dialog box](image)

4. Click **Yes** or **Yes to all** to start the zapping process and display the Zap Progress dialog box.

![Zap Progress dialog box](image)

**Note:** The file name and zap status display in the Zap Progress panel and in the Event Log of the SecretAgent Explorer Display Area panel.

5. Click the **Close Window** to display the SecretAgent 5 Explorer window.
Working with Office Suite Applications

SecretAgent 5 works with a wide range of popular application programs that run on Windows operating systems. SecretAgent offers seamless integration with Microsoft Office Suite (Word, Excel, and PowerPoint) for Windows 95, 98, 2000, and NT 4.0.

The procedures that follow describe the general processes for encrypting and decrypting a Word, Excel, or PowerPoint file. You can activate SecretAgent by clicking the SecretAgent icon on the Word, Excel, or PowerPoint toolbar or using the **SA5 Encrypt** menu option in the Tools Menu in Word, Excel, and PowerPoint.

**Encrypting a Document**

When you encrypt a document using SecretAgent 5, it is saved as a filename [doc, xls, or ppt].sa5 file with the SecretAgent 5 icon. The following procedure assumes you have a document open and the document was previously saved.

⇒ **To encrypt a document:**

1. Select **Tools, SA5 Encrypt...** from the Tools menu.
2. If more than one personality is available, the SecretAgent 5 Personality Manager dialog box will open. Select the desired personality in the list and click **Login**. If only one personality is available, you will not see the Personality Manager dialog box.
2. When the Encryption dialog box appears, confirm the Archive Type and Options settings. Then select one or more names in the Available Certificates panel and click >> to copy them to the Selected Recipients panel.

3. Click OK to close the Word document and encrypt the saved file. The encrypted file is placed in the default ciphertext output folder for the active personality.

Decrypting a Document

When you encrypt a document using SecretAgent 5, it is saved as a filename[doc, xls, or ppt].sa5 file and bears the SecretAgent 5 icon. The following procedure shows how to decrypt a previously encrypted document.

✦ To decrypt a document:

1. Run SecretAgent 5 and click the Decrypt button (or select Decrypt... in the adjacent drop-down menu), to display the Select Files to Decrypt dialog box.
2. Navigate through folders and files and click on the file to decrypt.

3. Click **Open** to display the Enter Password dialog box.

4. Type the user password in the Password text box.

5. Click **OK** to decrypt the document and place the plaintext version in the designated directory. Open the decrypted document in the appropriate application.

**Exiting SecretAgent 5**

You can exit SecretAgent 5 at any time without affecting other applications you may have running. If you have the auto-encryption option turned on, the files you have specified will automatically be encrypted and their corresponding source files will be automatically zapped. The next time you start SecretAgent 5, these encrypted files will be automatically decrypted when you enter your password.
To exit from SecretAgent 5 Explorer view:

1. Click the Close icon or the ‌‌located at the top right-hand corner of the SecretAgent 5 Explorer window.

To exit from System Tray view:

1. Click the SecretAgent 5 icon located in the System Tray to display the menu.
2. Select Close SecretAgent 5 from the menu.

To exit from SecretAgent Toolbar view:

1. Click the ‌‌located at the top right-hand corner of the Toolbar.
CHAPTER 4

SecretAgent 5 Explorer

The SecretAgent 5 Explorer is the primary work site for SecretAgent 5 activities. The Explorer is similar in operation to Windows Explorer. From the SecretAgent 5 Explorer window, almost all of the SecretAgent functions can be located, started, and completed. Two other ways to access SecretAgent 5 are available—a floating toolbar and an icon on your Windows System/Task Bar. These options make it easy to leave SecretAgent open while you work in other applications.

This chapter covers:

♦ Elements and functions of the SecretAgent 5 Explorer window
♦ Procedures for using SecretAgent 5 Explorer for:
  - Encrypting Files
  - Decrypting Files
  - Signing Files
  - Verifying Files
  - Zapping Files
  - Auto-Encrypting and Auto-Decrypting Files

For additional information about the user personalities and preferences options, see Chapter 5 Personality Manager. For additional information about the SecretAgent 5 certificates, see Chapter 6 Certificate Explorer.
SecretAgent 5 Explorer Window

The SecretAgent 5 Explorer window consists of:

- Title bar
- Tool/Menu bar
- Go To bar
- All Folders panel
- Contents panel
- Display Area panel
- Display Area tabs

The following subsections describe each element and function of the SecretAgent 5 Explorer window.
Tool/Menu Bar

The SecretAgent 5 Tool/Menu bar contains ten options (five drop-down menus and five tools). Each option is identified by an icon and a name. The following table describes the icon, name, and function of each Tool/Menu bar element.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Description or Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt</td>
<td>Click this icon to access the file selection dialog for encryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the arrow next to the icon to display menu options used to encrypt files</td>
</tr>
<tr>
<td>Decrypt</td>
<td>Click this icon to access the file selection dialog for decryption</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the arrow next to the icon to display menu options used to decrypt files</td>
</tr>
<tr>
<td>Sign</td>
<td>Click this icon to access the file selection dialog for signing</td>
<td></td>
</tr>
<tr>
<td>Verify</td>
<td>Click this icon to access the file selection dialog for signature verification</td>
<td></td>
</tr>
<tr>
<td>Zap</td>
<td>Click this icon to access the file selection dialog for zapping</td>
<td></td>
</tr>
<tr>
<td>Certificates</td>
<td>Click this icon to start Certificate Explorer</td>
<td></td>
</tr>
<tr>
<td>Personality</td>
<td>Click this icon to access the options dialog for the active user personality</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the arrow next to the icon to display menu options used to manage or change personalities</td>
</tr>
<tr>
<td>Views</td>
<td>Click this icon to change the way items in the contents panel area are displayed (large icons, small icons, list, or details)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click the arrow next to the icon to display menu options used to adjust display parameters</td>
</tr>
<tr>
<td>Icon</td>
<td>Name</td>
<td>Description or Function</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------------------</td>
</tr>
</tbody>
</table>
| ![Help icon](image) | Help | Click this icon to access on-line help  
Click the arrow next to the icon to display menu options used to obtain on-line and web-based help |
| ![Close icon](image) | Close | Click this icon to exit SecretAgent 5 |

**Encrypt Menu**

The Encrypt menu options allow you to encrypt one or more files, create a single archive, or create a self-extracting archive. Click on the arrow to display the menu options.

The Encrypt menu options are:

**Encrypt** Choose a file or files to encrypt. The encrypted file extension is changed to a SecretAgent file (*.sa5) and the file is placed in either the default or a user selected folder to await further action.

**AutoEncrypt Now** Activate automatic encryption options and encrypt the selected AutoEncrypt folder(s).

Note: As an alternative to using the Encrypt menu option, click on the Encrypt icon to directly access the dialog box used to select files for encryption.
**Decrypt Menu**

The Decrypt menu options allow you to decrypt one or more files; decrypt and verify the digital signature on one or more files; or automatically decrypt AutoEncrypt files. Click on the arrow to display the menu options.

The Decrypt menu options are:

**Decrypt**
Choose one or more encrypted files to decrypt. Decrypted files are converted to a plain text file and placed in either the default or a user selected folder.

**AutoDecrypt Now**
Automatically decrypt the selected folder content and restore the plain text files in the folder.

*Note: As an alternative to using the Decrypt menu option, click on the Decrypt icon to directly access the dialog box used to select files for decryption.*

**Sign, Verify, and Zap Tools**

These tools are used to sign, verify, or zap (delete) encrypted files. Click on a tool icon to display a standard Windows dialog box that allows you to locate and select specific folders and files, and to sign, verify, or zap files.
The Select Files To Sign dialog box is an example.

Once you locate a file to sign, verify, or zap, select it and make sure its file name displays in the File name text box. Then click Open to continue the operation (sign, verify, or zap).

**Certificate Explorer**

Certificate Explorer allows you to manage connections with multiple certificate databases from which your correspondents’ certificates can be drawn when needed by SecretAgent. See Chapter 6 *Certificate Explorer* for further information.

Click on the Certificate icon to run Certificate Explorer.
**Personality Menu**

The Personality menu options allow you to review the properties assigned to a user or change the personality profile of a user. Click on the arrow to display the menu options. See Chapter 5 *Personality Manager* for information on establishing and modifying user personalities.

The Personality menu options are:

- **Preferences**
  Display the Personality Preferences dialog box for the current user and change the personality settings.

- **Manage**
  Display the SecretAgent 5 Personality Manager dialog box in order to logoff as the current user and log in as another user.

Note: As an alternative to using the Personality, Preferences menu option, click on the Personality icon to directly access the dialog box used to change personality settings.

**Views Menu**

The Views menu options allow you to select a viewing option for working in SecretAgent 5—Explorer, Toolbar, or System Tray. It also allows you to change the display mode (large icons, small icons, list, or details) for the Contents panel.
The Views menu options are:

**Explorer**
Display SecretAgent 5 in the full Explorer Window mode.

**Toolbar**
Display SecretAgent 5 as a floating toolbar.

**System Tray**
Display SecretAgent 5 as an item on the System tray (bottom of screen with pop-up menu).

**Large Icon**
Display the folders and files in the Contents panel as large icons.

**Small Icon**
Display the folders and files in the Contents panel as small icons with names.

**List**
Display the names of folders and files in the Contents panel as a list.

**Details**
Display folder and file details such as the date created or last modified as a list in the Contents panel.

Note: As an alternative to using the Views menu options, click on the Views icon to change the Contents panel to display large icons, small icons, list, or details.
Help Menu

The Help menu options provide information about SecretAgent 5 and sources for additional help and technical support. Click on the arrow to display the menu options.

The Help menu options are:

**Help Topics**  Display on-line help.

**Support on Web**  Access on-line help through the web.

**About SecretAgent 5**  Display information about this version of SecretAgent.

Note: As an alternative to using the Help menu options, click on the Help icon to access Help Topics: SecretAgent index.

Close Tool

The Close tool logs the user off, closes SecretAgent 5, and exits the program.
Go To Bar

The Go To bar provides shortcuts to your default ciphertext and plaintext folders and to the SecretAgent clipboard.

| Go To Cipherpath | Go To Plainpath | Open Clipboard Viewer |

Go To Cipherpath  Navigates to the default ciphertext folder for the active personality.

Go To Plainpath  Navigates to the default plaintext folder for the active personality.

Open Clipboard Viewer  Displays the SecretAgent Clipboard Viewer.
The Clipboard Viewer allows you to encrypt and decrypt information that has been placed in the Windows clipboard or copied directly into the SecretAgent Clipboard Viewer. For example, you could select and copy text from a Word document and place it as plaintext on the SecretAgent Clipboard Viewer. Then, use SecretAgent to encrypt the content in the clipboard, copy the ciphertext from the clipboard, and paste it into the Word document or an e-mail.

All Folders and Contents Panels

The All Folders and the Contents panels of the SecretAgent 5 Explorer window provide access to all of your system drives, folders, and files. SecretAgent 5 Explorer has the same features as Windows Explorer. It allows you to navigate through folders and files, drag-and-drop files, copy and delete files, and open a file within another application by double-clicking directly from the Explorer window.
Display Area Panel

The Display Area panel of the SecretAgent 5 Explorer window consists of a large horizontal display area and three tabs at the bottom of the window. Select a tab to bring related information in the Display Area.

To hide the Display Area panel, click on the triangle in the lower left-hand corner of the window. The Event Log display is an example.

The three Display Area panel tabs are:

Selected Files Display a list of all currently selected files. Drag-and-drop files into this panel to store for later action (encrypt, decrypt, sign, verify, and zap).

AutoEncrypt List Display a list of all the folders selected for automatic encryption and decryption using the SecretAgent 5 AutoMagic Encryption.

Event Log Display a log that shows all SecretAgent events for this user during this session, or as otherwise specified in the user personality.
Working with SecretAgent 5 Explorer

SecretAgent 5 is a versatile tool that allows the user to work with the program in several different ways. You can encrypt, decrypt, sign, verify, or zap a file by first selecting that file and then clicking an icon on the SecretAgent 5 Toolbar. Alternately, you can use the Toolbar menu options to initiate those operations. You can even drag a file from any Windows donor application and drop it onto an icon on the Toolbar. Use whichever of these methods you find most convenient in a given situation.

Hint: To quickly initiate an operation, select a file in the Contents Display in SecretAgent 5 Explorer view (or in Windows Explorer), drag the file over to the SecretAgent toolbar and drop it onto the Encrypt, Decrypt, Sign, Verify, or Zap icon.

Encrypting Files

Encryption is a process that converts data from a readable (usable) form into a scrambled (unusable) form. In order to use the encrypted data, a user must supply the password (or key) required to convert the unreadable file back to some its original, usable form. Encryption ensures privacy.

SecretAgent 5 offers a wide variety of customizable encryption settings. The default encryption settings for a given personality are set using the Personality Preferences dialog. See Chapter 5 Personality Manager for additional information.

The following procedure explains how to encrypt one or more files using SecretAgent 5 menu options. Alternately, files have been selected, you may click on the Encrypt icon in the toolbar to begin the default encryption process.
To encrypt one or more files:

1. Select **Encrypt, Encrypt...** on the Tool/Menu. If you are using Explorer view and have already selected files to encrypt, skip to step 3. Otherwise, the Select Files to Encrypt dialog box will appear.

2. Navigate through your folders and select one or more files. Their names will be placed the File name text box. Click **Open** to continue.

   Note: To select more than one file to encrypt, hold the **Ctrl** key down as you click each of their filenames.

3. The Encryption dialog box will appear.

4. Choose one of the three available output Archive Types by setting the corresponding radio button:
Separate files means that all input files will be placed into individual (.sa5) ciphertext output files.

A single archive means that the ciphertext produced from all input files will be combined into a single (.sa5) output file. (Of course, these first two options are the same if there is only one input file.)

A self-extracting archive means that the ciphertext will be combined into a single Windows executable (.exe file).

5. If you chose A self-extracting archive, skip to step 7 below. Otherwise select a recipient from the Available certificates panel and click the >> button to place it in the Selected recipients panel.

  Note: Since for self-extracting archives only a symmetric cipher is used to protect the data, you will not be allowed to select recipients.

6. Repeat step 5 until all of the desired recipients are listed in the Selected recipients panel.

  Note: For group or network installations using the SecretAgent Key Recovery feature, designated Key Recovery Agents will be automatically listed in the Selected recipients panel. These recipients cannot be removed by the user.

7. (Optional) Check any of the available encryption Options that you desire. Which settings are available will depend upon the Archive Type choice you made in step 4 above.

  Sign plaintext will cause your digital signature over the input files to be included in the archive. (This signature will be automatically validated whenever a designated recipient decrypts the archive. This choice is not available for self-extracting archives.)

  Zap source files will cause the input files to be securely erased once they are encrypted.
Send via e-mail directs SecretAgent to send the output ciphertext archive to each recipient for whom you have an email address. (This choice is currently not available for self-extracting archives.)

8. If you selected A single archive or A self-extracting archive as the Archive Type, enter a name for the output file in the Archive Name field or simply accept the (rather generic) suggested filename. If you selected Separate files, the output files will be named automatically.

9. Click OK to start the encryption process. If you selected A single archive or A self-extracting archive as the Archive Type, continue with step 10. If you selected A self-extracting archive, you will be prompted to enter a password for the archive:

```
Please enter a passphrase for the self-extracting archive:

[Text box]

OK  Cancel
```

Type a secure passphrase of between eight and forty characters into the text box and click OK.

Note: Do NOT use your login password! Choose another, unrelated passphrase. This passphrase must be supplied (out of band!) to anyone to whom the self-decrypting .exe file is sent. When they run the .exe, they will be prompted to enter this passphrase so that the file may decrypt itself.
10. The Encrypt Progress dialog box will appear.

![Encrypt Progress dialog box]

When the encryption process is complete, click **Close Window** to display the SecretAgent 5 Explorer window or simply wait until it closes automatically.

**Note:** The File Name and Encrypt status of each input file is displayed in the lower Encrypt Progress panel. This information is also copied into the Event Log tab of the SecretAgent Explorer Display Area panel so that you can read it even after the Encrypt Process dialog closes.
Decrypting Files

Decryption is a process that converts an encrypted file back to its original form (plain text or readable text). In order to decrypt a file, the system must recognize the type of encryption that was performed and reverse the encryption process (when a valid password is entered).

SecretAgent 5 offers a wide variety of customizable decryption settings. The default decryption settings for a given personality are set using the Personality Preferences dialog. See Chapter 5 Personality Manager for additional information.

The following procedures provide instructions for decrypting one or more files. The procedures use the menu options. As an alternative, click on the Decrypt icon to begin the process.

To select and decrypt a file:

Note: This procedure may also be used to decrypt an archive.

1. Click the Decrypt icon on the Tool/Menu bar to display the Select Files To Decrypt dialog box.

2. Navigate through the folders and files. Click on the desired file to place its name in the File name text box.

Note: To select more than one file to decrypt, hold the Ctrl key down as you click on the desired files.
3. Click **Open** to display the Enter Password dialog box.

![Enter Password dialog box]

4. Type your password in the Password text box.

5. Click **OK** to begin the decryption process and display the Decrypt Progress dialog box.

![Decrypt Progress dialog box]

Note: The file name, decryption status, and plaintext file name display in the Decrypt Progress panels and in the Event Log of the SecretAgent Explorer Display Area panel.

6. (Optional) Select the Plaintext File and click **Open File** to launch the application in which the file was created and open the file.

7. Click **Close Window** to display the SecretAgent 5 Explorer window.
Signing Files

When you sign a file, your private key is used to wrap a fingerprint of the file’s data. Using the public key in your certificate, any recipient of the data and can validate this signature and be assured that you were the signer. In this process the integrity of the data is also verified.

To sign a file:

1. Click the Sign icon on the Tool/Menu bar to display the Select Files To Sign dialog box.

2. Navigate through the folders and files. Click on the desired file to place its name in the File name text box.

   Note: To select more than one file to sign, hold the Ctrl key down as you click on the desired files.

3. Click Open to display the Enter Password dialog box.

4. Type the user password in the Password text box.
5. Click **OK** to begin the signing process and display the Sign Progress dialog box.

![Sign Progress dialog box]

Note: The file name and sign status display in the Sign Progress panel and in the Event Log of the SecretAgent Explorer Display Area panel.

You may also instruct SecretAgent 5 to always add a signature to plaintext or e-mail by setting that option in your user personality. See Chapter 5 *Personality Manager* for additional information.

### Verifying Signatures

Verifying a file means that the digital signature associated with it is checked to establish the authenticity of the sender and to ensure the recipient that the file has not been modified.

**To validate a signature:**

1. Click the **Verify** icon on the Tool/Menu bar to display the Select Files To Validate Signature dialog box.

![Select Files To Validate Signature dialog box]
2. Navigate through the folders and files. Click on the desired file to place its name in the File name text box.

   Note: To select more than one file to verify, hold the **Ctrl** key down as you click on the desired files.

3. Click **Open** to start the verifying signature process and display the Verify Progress dialog box.

   ![Verify Progress dialog box](image)

   Note: The file name, verification status, and plaintext file name display in the Verify Progress panels and in the Event Log of the SecretAgent Explorer Display Area panel.

4. (Optional) Select the Plaintext File and click **View Signature** to display the Signature dialog box and see information about the signer.
5. Click **Close** or **Close Window** to display the SecretAgent 5 Explorer window.

### Zapping Files

The Zap function of SecretAgent 5 securely and permanently deletes a file from your hard drive. There is no way to recover a zapped file. Use the following procedure to zap a file in the SecretAgent 5 Explorer window.

✦ **To zap a file:**

1. Click **Zap** on the Tool/Menu bar to display the Select Files to Zap dialog box.
2. Navigate through the folders and files. Click on the desired file to zap.

   Note: To select more than one file to zap, hold the Ctrl key down as you click on the desired files.

3. Click **Open** to display the Confirm File Zap dialog box.

![Confirm File Zap dialog box](image)

4. Click **Yes** or **Yes to all** to start the zapping process and display the Zap Progress dialog box.

![Zap Progress dialog box](image)

   Note: The file name and zap status display in the Zap Progress panel and in the Event Log of the SecretAgent Explorer Display Area panel.

5. Click **Close Window** to display the SecretAgent 5 Explorer window.
Auto-Encryption and Auto-Decryption

The SecretAgent 5 AutoMagic Encryption option allows you to specify certain folders that are to be automatically decrypted whenever you login to SecretAgent and then re-encrypted when you exit SecretAgent. This process is largely transparent to the user.

AutoMagic Encryption is controlled by settings on the Encryption tab of the Personality Preferences dialog box. Each user who desires to use these features must first enable them and then select the folder(s) to be auto-encrypted/decrypted. Use the following procedures to configure the SecretAgent 5 AutoMagic Encryption options.
To enable AutoMagic Encryption:

1. Open SecretAgent in Explorer View and make sure that you are logged using the personality for which you want to configure AutoMagic. If necessary, use the Personality Manager to change the active personality.

2. Select **Personality, Preferences** from the Menu bar to open the SecretAgent 5 Personality Preferences dialog box and select the **Encryption** tab:

3. Turn on the desired AutoMagic Options settings and click **OK** to accept your changes.
4. When you return to the SecretAgent 5 Explorer window, open the **AutoEncrypt List** tab in the lower Display Area and drag and drop folders to be auto-encrypted into it:

Now, whenever you close the SecretAgent 5 application, all files in the folders you placed in the AutoEncrypt List will be automatically encrypted:
Similarly, each time you login to SecretAgent 5 with this personality, all files in its AutoEncrypt List will be automatically decrypted.
To disable AutoMagic Encryption:

1. Open SecretAgent in Explorer View and make sure that you are logged using the personality for which you want to configure AutoMagic. If necessary, use the Personality Manager to change the active personality.

2. Select Personality, Preferences from the Menu bar to open the SecretAgent 5 Personality Preferences dialog box and select the Encryption tab:

3. Uncheck the desired AutoMagic Options settings and click OK to accept your changes.
SecretAgent 5 requires each user to establish and maintain a user personality. The personality contains user-selected preferences and settings that affect both the way the user interacts with SecretAgent and the way SecretAgent works with the user’s files. The user personality options are in effect each time a user works with SecretAgent 5. If specific user personality options are not selected, the program uses the default options.

This chapter covers:
- User personality options and preferences
- Procedures for using the Personality Manager for:
  - creating a user personality
  - modifying a user personality
  - removing a user personality

**Personality Options and Preferences**

Each user personality consists of multiple options and preferences that SecretAgent 5 uses to identify and customize the encrypt/decrypt process for each user.

The default options are used for each new user unless specific options are selected to customize the user personality. You may change or modify your personality options or preferences at any time. User personality options are customized in the Personality Preferences window.
There are seven tabs available from the Personality Options window:

- General
- Encryption
- Algorithms
- Credentials
- Output
- Plug-ins/Macros
- Events

**General Tab**

The General tab allows you to select SecretAgent 5 operating preferences. Observe the special warnings before changing any of the default options.

![Personality Options](image)
The SecretAgent 5 General options are:

**Cache password for “x” minutes**
Select this option to cache passwords for a user-determined number of minutes. Password caching allows you to temporarily store your password in memory so that you can encrypt, decrypt, and sign archives without typing your password each time. A check mark indicates this option is selected. Click the arrows to increase or decrease the time allotted.

---

**WARNING!**
Password caching can be used to expedite certain redundant processes. The password-caching scheme used in SecretAgent 5 is not secure and should not be used unless you are sure that the security of the program cannot be comprised.

**Close progress windows after “x” seconds**
Select this option to display a progress window for a user-determined number of seconds. A check mark indicates this option is selected. Click the arrows to increase or decrease the number of seconds you want the window to display.

**Encryption Tab**
The Encryption tab allows you to select encrypted document formats and related actions. It permits you to automatically encrypt and save when you exit SecretAgent 5 and automatically decrypt files when you log in.
The SecretAgent Encryption options are:

**Encrypt document as**

Use this drop-down list box to select the type of encrypted file you want to create. The options are:

- **single document archives (*.sa5)**
  Encrypt and save the file as one document with the extension .sa5.
  Example: (filename)[doc].sa5

- **multiple document archives (*.sa5)**
  Encrypt and save more than one file at the same time as an archive with the extension .sa5.
  Example: (archivename).sa5

- **self-extracting archives (*.exe)**
  Encrypt and compress the file(s) as a single self-extracting file with the extension .exe.
  Example: (archivename).exe
Default Settings
Select one or more of the following options. A check mark indicates an option is selected:

Sign plaintext
Digitally sign the plaintext file prior to encryption.

Zap sources
Completely remove the original source file from the computer’s hard drive after encryption.

Mail
Immediately e-mail an encrypted (ciphertext) file to all listed e-mail addresses after a source (plaintext) document is encrypted.

Always include me as a recipient for archives
Automatically include the originator (the currently logged-in personality) as a recipient.

AutoMagic Options
AutoMagic automatically decrypts selected files at login and encrypts selected files at exit. A check mark indicates an option is selected. The options are:

Encrypt selected files on exit
Select this option to encrypt previously selected folders when you exit SecretAgent.

Decrypt selected files on login
Select this option to decrypt previously selected folders when you log into SecretAgent.

WARNING!
Files may not be secure if Windows is not shut down properly.
Algorithms Tab

The Algorithms tab allows the advanced user to select specific algorithms and encryption schemes that SecretAgent 5 will apply to your documents. Use the default settings.

The Algorithm options are:

Ciphers

Use the drop-down list boxes to select the desired encryption algorithm for each of the three types of ciphertext archives: SA5 archives, Automatic encryption, and Self-extracting.

SA5 archives (*.SA5)

Select the encryption algorithm that will be used to produce .sa5 archives from the list of available ciphers: DES (CBC), DES3 (CBC), DESX (CBC), and EA2 (CBC).
Automatic encryption (*.SAA)
These ciphertext files are produced automatically when you exit SecretAgent and decrypted when you start the next session if AutoMagic Encryption is enabled. Currently DESX is the only symmetric cipher that can be used for this file type.

Self-extracting (*.EXE)
This option applies a symmetric cipher to one or more plaintext files combining the ciphertext into a single Windows executable (with an .exe filename extension). This file decrypts itself when you run the executable and supply the proper password. Currently RC4 is the only symmetric cipher that can be used for this file type.

Formats
Use the drop-down list boxes to select the algorithm that will be applied to each document during:

Compression
Compressing plaintext before encrypting it can result in a smaller ciphertext file and faster processing times. However, some files (such as certain graphics files) do not compress very well and attempting to compress them is simply a waste of time. The SecretAgent compression choices are None and LZSS (a variant of Lempel-Ziv).

Encoding
Most modern transmission protocols support arbitrary binary files, but for some purposes it is desirable to produce printable ASCII characters. To support both scenarios, SecretAgent offers two encoding options: Binary (i.e., no encoding) and Base64 encoding.

Test Engine
Click this button to run an internal test suite on the available ciphers and to display the Engine Algorithm Test Results dialog box.
**Revert to Defaults**

Click this button to change all of the options on this tab to their original default settings.

**Credentials Tab**

SecretAgent 5 uses tokens such as certificates or smart cards to secure data. This tab provides information about the token currently in use and, if available, allows you to select another token.

Note: Contact your technical support representative if you need a specific token that was not supplied as part of SecretAgent 5. Additional tokens, if available, will be sent along with a simple install program that will automatically update your version of SecretAgent 5 and allow it to recognize the new token.

The token options and settings are:
Type Displays the currently used token.

Library Lists the path to the current token library.

Library version Lists the version number of the current token library.

Driver version Lists the current driver version used by your system.

Credential configuration information Provides a description of the attributes that can be configured.

Configure Click this button to access the Select Certificate dialog box from which you can select another user name from the list of users associated with the current certificate.

Output Tab

The Output tab allows you to select or indicate the output path and folders you want to use for both ciphertext and plaintext files.

Note: A ciphertext archive is created each time one or more documents are encrypted. The default destination for such archives is [SA5 folder]\[UserName]\Cipher. One or more plaintext files are produced each time an encrypted archive is decrypted. The default destination for plaintext files is [SA5 folder]\[UserName]\Plain.

The Output tab also allows you to select encrypted document formats and several other related actions.
The Output options are:

**Folder**

**Always use source folder**
Select this option to always save ciphertext (encrypted) and plaintext (decrypted) files in the same folder in which the original document file resides. A check mark indicates this option is selected.

**Ciphertext output path**
Indicates the output path you want to use for all of your ciphertext (encrypted) files, if other than the default location. The default location is [SA5 folder]\[UserName]\Cipher. Use the Browse button to locate an alternate folder or type the name of the folder you want to use.
Plaintext output path
Indicates the output path you want to use for all of your plaintext (decrypted) files, if other than the default location. The default location is [SA5 folder]\[UserName]\Plain. Use the Browse button to locate an alternate folder or type the name of the folder you want to use.

File Overwrite
Select one of these options to manage the ability of SecretAgent 5 to overwrite files. A dot indicates an option is selected. The choices are:

**Never**
Select this option to prevent SecretAgent 5 from overwriting an existing file. For example, if you select this option and attempt to encrypt a plaintext document more than once and save the resulting ciphertext file in the same location each time, the system will abort the process.

**Always**
Select this option to permit SecretAgent 5 to always overwrite a plaintext document or a ciphertext archive. For example, if you select this option and attempt to encrypt a plaintext document more than once and save the resulting ciphertext file in the same location each time, the system will overwrite the first ciphertext file and save only the latest version.

**Prompt**
Select this option to allow SecretAgent 5 to prompt for permission to overwrite a file before proceeding. For example, if you encrypt a plaintext document more than once and save the resulting ciphertext file in the same location, a dialog box will prompt you to overwrite the previous version,
save the new file with a new name, or abort the process.

**Plug-ins/Macros Tab**

The Plug-ins/Macros tab allows you to indicate how SecretAgent will operate when you sign or send e-mail, or use the Certificate Explorer to locate missing certificates.

![Personality Options For Bob Carlson](image)

The SecretAgent 5 Plug-ins/Macros options are:

**Sign e-mail messages by default**

Enables the Sign checkbox (by default) when composing an e-mail message.

**Encrypt e-mail messages by default**

Enables the Encrypt checkbox (by default) when composing an e-mail message.
Launch Certificate Explorer to locate missing certificates
Launches the Certificate Explorer to locate any certificates for recipients not in the Personal Certificates database. If this option is not selected and a recipient’s certificate cannot be found, the recipient will not be included in the e-mail message.

Always include me as a recipient for encrypted e-mail
Automatically includes the originator (the currently logged-in personality) as a recipient of the e-mail message.

Events Tab
The Events tab allows you to select the types of events that will be recorded in the Event Log of the SecretAgent 5 Explorer window. The log records and displays all the events for the types selected.
Select one or more of the following options. A check mark indicates an option is selected:

**Encrypt** Displays the date, time, input and output file name and path, and status of recently encrypted files.

**Decrypt** Displays the date, time, input and output file name and path, and status of recently decrypted files.

**Sign** Displays the date, time, input and output file name and path, and status of recently signed files.

**Verify** Displays the date and time of all verification activities.

**Zap** Displays the date, time, input and output file name and path, and status of recently zapped files.

**Certificates** Displays the date and time of all certificate verification activities and properties information of any certificate created or modified.

**Engine** Displays the date and time of encryption engine activities such as functionality queries.

**Password** Displays the date and time of all password verification activities.
Managing Multiple Personalities

When you begin a SecretAgent 5 session, you are prompted to select a personality from the list of Available SecretAgent 5 Personalities and login. If you do not see the desired Personality in the list, you may want to create a new Personality.

This section provides procedures for:
- Creating a new user personality
- Modifying a user personality
- Removing a user personality

Creating a New User Personality

This procedure assumes you are working in the SecretAgent 5 Explorer window and requires that you select specific personality options. If you do not know which options to select, use the default values.

Each user personality is attached to a certificate. You must have a certificate in the Personal Certificate folder to complete this procedure. If you do not have a certificate, the procedure directs you to run Certificate Explorer to import or generate the required certificate.

To create a new user personality:

1. Select Personality, Manage from the Tool/Menu bar to display the SecretAgent 5 Personality Manager dialog box.
2. Click **New** to start the New Personality Wizard.

3. Type the name for this personality in the Personality Name text box.

4. Click **Next** to display the Associate Credentials dialog box.
5. Select the credentials from the list of available credentials to use when encrypting, decrypting, and signing with this personality.

6. Click **Next** to display the Select Certificate dialog box.

7. Select a name from the list of names in the Common Name (CN) text box and review the description in the Certificate Information text area. Click on the desired certificate to make sure it is selected.
Note: If no appropriate certificate is available, click **Launch Certificate Explorer** to display the Certificate Explorer window. See Chapter 6 *Certificate Explorer* for information on creating a new certificate.

8. Click **OK** to display the New Personality Wizard’s Set Default File Locations dialog box.

![New Personality Wizard Set default file locations dialog box](image)

9. Select the location of the folders where you want to store the ciphertext and plaintext documents. Click **Select**... to navigate through the folders.

10. Click **Next** to display the New Personality Wizard’s Finished! dialog box.

![New Personality Wizard Finished! dialog box](image)
Note: Click **Configure** to set your user personality options and preferences.

11. Click **Finish** to display the SecretAgent 5 Personality Manager dialog box with the new user’s name in the Available SecretAgent 5 Personalities area.

![SecretAgent 5 Personality Manager dialog box](image)

12. Click **Close** to return to the SecretAgent 5 Explorer window.

### Modifying a User Personality

Use this procedure to modify your user personality. This procedure begins in the SecretAgent 5 Explorer Window and assumes you want to modify only your user personality.

**To modify an existing Personality:**

1. Select **Personality, Preferences...** from the Tool/Menu bar to display the SecretAgent 5 Personality Preferences dialog box.
2. Select the **General** tab to display the currently selected and available options. Make desired changes on this tab.

![Personality Options for Bob Carlson](image)

3. Select the **Encryption** tab to display the currently selected and available file options. Make desired changes on this tab.

4. Continue selecting tabs (Algorithms, Credentials, Output, and Plug-In Macros) and making desired changes.

---

**Note:** See the Personality Options and Preferences section at the beginning of this chapter for information on the fields and options available under each of the seven tabs in this dialog box.

5. Click **OK** to accept the settings and changes on all of the tabs in the Personality Preferences dialog box.
Removing a User Personality

Use this procedure to remove a user personality. This procedure begins in the SecretAgent 5 Explorer Window and assumes you want to remove a personality.

To remove an existing Personality:

1. Select **Personality, Manage** from the Tool/Menu bar to display the SecretAgent 5 Personality Manager dialog box.

![SecretAgent 5 Personality Manager](image)

2. Select the name of the user personality from the list of Available SecretAgent 5 Personalities.

3. Click **Delete** to display the Confirm Delete dialog box.

![Confirm Delete](image)

4. Optionally select one or more of the folders to be removed and then click **Yes** to confirm the deletion.
Certificate Explorer is the SecretAgent 5 component used to create personal certificates and/or certificate requests. Certificate Explorer also manages your “connections” to those local or remote certificate databases to which access is required by SecretAgent.

You can open Certificate Explorer by selecting the Certificate Explorer item in your Window’s Start | Programs | SecretAgent 5 menu. You can also launch it whenever you’re working in SecretAgent 5 by simply clicking the Certificate icon on the Tool/Menu:

This chapter covers:

- Certificates and keys
- Elements and functions of the SecretAgent 5 Certificate Explorer window
- Using Certificate Explorer for:
  - Creating self-signed certificates
  - Creating certificate requests
  - Importing certificates
  - Exporting certificates
  - Sending certificates
  - Deleting certificates
  - Changing certificate properties
- Components of the New Certificate Wizard
What is a Certificate?

A certificate is a document to which a digital signature has been affixed in order to affirm its authenticity. A public key certificate is issued (i.e., digitally signed) by an authority wishing to bind a public key to the identity of a particular subject. Public key certificates (the only kind we will discuss in this manual) allow the originators of confidential messages to be sure that only their intended recipients can read them. They also allow those recipients to verify the digital signatures of the originator. SecretAgent supports self-signed certificates (to which a somewhat limited level of trust can be assigned) as well as the standard X.509 certificates issued by most well-respected certificate authorities.

Secret Keys

Traditional cryptography is based on the sender and receiver of a message knowing and using the same secret key. The sender uses the secret key to encrypt the message, and the receiver uses the same secret key to decrypt the message. This method is also known as symmetric cryptography due to the necessity of having the same key at both ends of the communications channel.

Public and Private Keys

The main problem with a single key system is in getting the sender and receiver to agree on the key without anyone else discovering what it is. Public key cryptography solves this problem by not requiring the a priori exchange of keys before secure communications can be initiated. In this system, each person possesses a pair of keys—a public key and a private key. The public key is freely and widely disseminated; while the private key is kept totally secret.

The originator of a confidential message sends it to its intended recipient wrapped in that recipient’s public key and they rest secure in the knowledge that the message can then only be decrypted with that recipient’s private key. The security of these communications depend on the authenticity of the public keys and that is exactly what certificates provide.
Certificate Explorer Window

This section describes each element of the SecretAgent 5 Certificate Explorer window. The Certificate Explorer window consists of:

- Title bar
- Tool/Menu bar
- Available Connections panel (left column)
- Contents panel
- Status bar
Tool/Menu Bar

The Tool/Menu bar is located at the top of the Certificate Explorer window. It has three options: Views, Help, and Close.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Name</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Views Icon]</td>
<td>Views</td>
<td>Click this icon to change the display mode for the Contents panel (large icons, small icons, lists, or reports) Click the arrow next to the icon to display menu options used to change the views</td>
</tr>
<tr>
<td>![Help Icon]</td>
<td>Help</td>
<td>Click this icon to access on-line help for Certificate Explorer Click the arrow next to the icon to display menu options used to obtain on-line help for Certificate Explorer</td>
</tr>
<tr>
<td>![Close Icon]</td>
<td>Close</td>
<td>Click this icon to exit Certificate Explorer</td>
</tr>
</tbody>
</table>

Available Connections Panel

The Available Connections panel provides access to one or more local or remote certificate databases. During installation SecretAgent creates a Personal Certificates database and, by default, any certificates or certificate requests (along with their associated encrypted private keys) are stored in it.

If your computer is on a network, other folders containing certificates may be available to you. Use the Connect button located above the Available Connections panel to establish a link to these other databases. If you no longer need a particular connection, highlight it and click Disconnect to remove that link.

- **Connect**: Click to create a new connection (to a local or remote database, or to an LDAP directory)
- **Disconnect**: Click to remove the selected connection from the Available Connections list.
Contents Panel

If the selected connection represents a file, the pathname of the folder is listed above the Contents panel. If the connection is to an LDAP directory, the IP address of the LDAP server is displayed. In either case, the Contents panel itself lists information on the certificates available via the selected connection. This information includes: the subject’s Common Name (CN) and Organization (O) and the certificate type.

For regular certificate database connections, you can create a new certificate, import or export a certificate, or send a certificate to someone by using the buttons located on the menu bar above the Contents panel.

New  Click to launch the New Certificate Wizard. The wizard guides you through the process of generating a self-signed certificate or certificate request (see New Certificate Wizard later in this chapter).

Import  Click to import a certificate contained in a file. The certificate may be your own or that of another individual.

Export  Click to export a certificate and store it in a file (which can later be sent to a correspondent).

Send To  Click to send a certificate to a correspondent via e-mail.

Validate  Click to check the validity of all certificates in the database.

For LDAP directories, you can view and modify the properties of the connection or start a new search using the Properties and New Search buttons located on the menu bar above the Contents panel.
Creating Certificates

Each user must possess at least one certificate in order to use SecretAgent 5. You can create a self-signed certificate by providing personal information and generating your own key pair, or you can generate a PKCS#10 certificate request and forward it to your local system administrator or to a commercial certificate authority.

This section provides procedures for:
- Creating a self-signed certificate
- Creating a certificate request

Creating a Self-Signed Certificate

This procedure assumes Certificate Explorer is running.

⇒ To create a self-signed certificate:

1. Select a certificate database and click the New button located above the Contents panel to launch the New Certificate Wizard.

Note: See New Certificate Wizard section at the end of this chapter for detailed information about the wizard.
2. Select the **Self-signed certificate** option and click **Next** to display the Enter Personal Information dialog box.

3. Type your personal information. Use the <tab> key to move the cursor to the next text box.

   Note: If you are part of a group or network installation, your name and organization information will display automatically.

4. Click **Next** to display the Select Algorithms dialog box.

   Note: The system will display a prompt if all fields in the Enter Personal Information text boxes are not completed. It is not necessary to complete all the fields, only the Common Name field is required. Click **Yes** to continue.
5. Select the type of key and message digest to be generated for the algorithm used on this certificate.

6. Click Next to display the Set Validity Period and Extensions dialog box.

7. Use the drop-down arrows to select validity dates: Not before and Not after. Then select the appropriate Key Usage options and Criticality setting for this certificate.
8. Click **Next** to display the Enter Your Password dialog box.

![Enter Your Password dialog box]

9. Type your password in the upper text box. Retype your password in the lower text box for confirmation.

   **Note:** Passwords are case sensitive. If you do not correctly confirm your password, you will be prompted to re-enter the password.

10. Click **Next** to display the Specify Disposition for Certificate/Request dialog box.

![Specify Disposition dialog box]

11. Select the **Store the certificate or request in the active certificate folder** option.
12. Click **Next** to display the Finished! dialog box.

![Finished! dialog box](image)

13. Click **Finish** to close the Certificate Wizard and return to Certificate Explorer.

---

**Creating a Certificate Request**

This procedure assumes Certificate Explorer is running.

⇒ **To create a certificate request:**

1. Select a certificate database and click the **New** button located above the Contents panel to launch the New Certificate Wizard.

Note: See New Certificate Wizard section at the end of this chapter for detailed information about the wizard.
2. Select the **PKCS#10 certificate request** option and click **Next** to display the Enter Personal Information dialog box.

3. Type your personal information. Use the <tab> key to advance to the next text box.

   **Note:** If you are part of a group or network installation, your name and organization information will display automatically.
4. Click **Next** to display the Select Algorithms dialog box.

   Note: The system will display a prompt if all fields in the Enter Personal Information text boxes are not completed. It is not necessary to complete all the fields, only the Common Name field is required. Click **Yes** to continue.

5. Select the type of key, message digest and encoding to be generated for the algorithm used on this certificate.

6. Click **Next** to display the Enter Your Password dialog box.
7. Type your password in the upper text box. Retype your password in the lower text box for confirmation.

   Note: Passwords are case sensitive. If you do not correctly confirm your password, you will be prompted to re-enter the password.

8. Click **Next** to display the Specify Disposition for Certificate/Request dialog box.
9. Select the **Store the certificate or request in the active certificate folder** option.

10. Click **Next** to display the Finished! dialog box.

11. Click **Finish** to close the Certificate Wizard and return to Certificate Explorer.
Importing, Exporting, and Sending Certificates

The Import, Export, and Send To options in Certificate Explorer are used to move certificates to and from files on your computer, move certificates to other computers on your network, and send certificates via e-mail to your correspondents. These options are only available when a certificate database Connection has been selected.

This section provides procedures for:
- Importing a certificate
- Exporting a certificate
- Sending a certificate

Importing a Certificate

The first step in importing a certificate is to select the source of the certificate. SecretAgent 5 supports the following actions:

- **Import a certificate file with optional private key**
  Use this action to import a certificate created on another system. Certificates (public keys) and private keys can be stored as files in the database, stored as a backup file, or sent to a user as a file.

- **Replace a certificate request with an issue certificate file**
  If you generate a certificate request, both the request and your private key are temporarily stored in the database pending issuance of your certificate. When a certificate authority returns your actual certificate, use this option to substitute it into the database in place of the request. The association between the certificate and your corresponding private key will be maintained.

- **Import a certificate from the selected hardware token**
  Use this action to read a certificate from a hardware token (e.g., a FORTEZZA cryptographic card) and
add it to your local certificate database. You must have the drivers for the token and reader, if any, installed on your system and also have the required SecretAgent 5 support for that token installed.

To start Certificate Explorer, you may click the Certificate Explorer button on SecretAgent’s toolbar or select the Certificate Explorer item in Window’s Start | Programs | SecretAgent 5 menu. The following steps assume Certificate Explorer is already running.

To import a certificate:

1. Select a certificate database and click the Import button located above the Contents panel to launch the Import Certificate Wizard.

2. Specify the source of the certificate to be imported and click Next to display the Select Certificate File dialog box.
3. Enter the full pathname of the certificate file or click **Select...** to display the Import Certificate From dialog box.

Navigate through your folders to locate the name of the certificate file to import. Select the certificate to display its name in the File name text box and click **Open** to return to the Import Certificate Wizard.
4. Click **Next** to import the certificate and display the Import Certificate Wizard’s Finished! dialog box.

5. Click **Finish** to return to Certificate Explorer.
Exporting a Certificate

The following steps assume Certificate Explorer is already running.

To export a certificate:

1. Select a certificate database and then select the certificate to export from the Contents panel in Certificate Explorer.

2. Click Export located above the Available Certificates Detail panel to display the Save Certificate As dialog box.

3. Navigate through the folders to locate the destination for the certificate. Type the name of the file containing the certificate in the File name text box.

4. Click Save to export the certificate and return to Certificate Explorer.

Note: For self-signed certificates, the Save Private Key As dialog box displays. Navigate through the folders to locate the destination for the private key. Type the name of the file containing the private key in the File name text box.
Sending a Certificate

The following procedure assumes Certificate Explorer is running. You can choose to save a certificate to a file in a specific folder or e-mail a certificate to a recipient.

To send a certificate to a file:

1. Select a certificate database and then select the certificate to save as a file from the Contents panel of Certificate Explorer.
2. Click Send to, File... located above the Available Certificate Detail panel to display the Save Certificate Entry As dialog box.
3. Navigate through your folders to find an appropriate target directory and enter a name for the certificate file.

4. Click **Save** to store the certificate in the specified file and return to Certificate Explorer.

To send a certificate to a recipient:

1. Select the certificate to be transmitted in the Available Certificates Detail panel of Certificate Explorer.

2. Click **Send to, Mail Recipient...** located above the Available Certificate Detail panel to display an e-mail form.

3. Complete the e-mail address information.

4. Click **Send** to launch your e-mail application, send the certificate, and return to Certificate Explorer.
Deleting a Certificate

The following procedure assumes Certificate Explorer is running.

To delete a certificate:

1. Select a certificate database and then select the certificate to delete from the Contents panel of Certificate Explorer.
2. Click the right mouse button to display the certificate context menu.
3. Select **Delete** to display the Confirm Delete dialog box.
4. Click **Yes** to delete the certificate and return to Certificate Explorer.
Modifying Certificate Properties

Use the following procedure to check your certificate properties and change your e-mail address or password. The procedure assumes SecretAgent 5 is running.

To change certificate properties:

1. Click the Certificate icon to start Certificate Explorer:

2. Select a certificate database in the Available Connections list and then double-click on the Common Name of the certificate to display its properties:

3. Click the General tab. To change the e-mail address, type the address in the E-Mail Address text box.
4. Click the **Extensions** tab to review the current Certificate Extensions.

![Certificate Properties window](image1)

5. Click the **Password** tab to display the Certificate Properties dialog box.

![Certificate Properties window](image2)

6. Type your current password. Type your new password. Retype your password for confirmation. Click **Change Password** to accept the changes.

7. Click **OK** to close the Certificate Properties dialog and return to Certificate Explorer.
**New Certificate Wizard**

The New Certificate Wizard assists you in the process of generating a certificate request or in creating a new self-signed certificate. This section describes the contents, dialog boxes, and field options you’ll encounter when running this wizard.

The New Certificate Wizard will lead you through the following actions:

- Providing personal identifying information
- Specifying the type of key to be generated
- Setting a validity period and usage extensions
- Setting a password to protect your private key
- Choosing handling options for your key material

**Entering Personal Information**

Provide the personal information requested in this dialog box to construct the X.509 distinguished name (DN) to be inserted into your certificate. Only the Common Name field must be completed. Fields left empty will be omitted when your certificate (or certificate request) is created. (In the case of a certificate request, the optional fields may be supplied by your system administrator, local registrar, or certificate authority.)
**Common Name (CN)**  [required]  
Typically your full name. Maximum 64 characters.

**Title (T)**  
Your title or position. Maximum 64 characters.

**Organization (O)**  
The name of your organization. Maximum 64 characters.

**Organizational Unit (OU)**  
The name of a subunit of the organization. 
Maximum two lines, 64 characters each.

**Locality/City (L)**  
The name of your locality or city. Maximum 128 characters.

**State/Province (SP)**  
The name of your state, province or other local government. Maximum 128 characters.

**Country (C)**  
Your country code. Maximum 2 characters.

**E-mail (EM)**  
Your e-mail address. Maximum 128 characters.
Selecting a Key Type

The Select Algorithms dialog box allows you to select the Key Type to be generated for the certificate and the Message Digest (or hash function) to be used. An additional Encoding option is available when creating a certificate request.

### Key Type

SecretAgent 5 can use four distinct types of public key algorithms for key agreement and sender authentication. Two or more key sizes are available for each type. The following table summarizes these options and lists the relevant standards.

<table>
<thead>
<tr>
<th>Key Type</th>
<th>Description</th>
<th>Key Sizes (bits)</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsa</td>
<td>DSA/Diffie-Hellman (FIPS 186, ANSI X9.30/42)</td>
<td>1024, 2048, or 512</td>
</tr>
<tr>
<td>ec2</td>
<td>Elliptic Curve (char. 2; ANSI X9.62/63, IEEE P1363)</td>
<td>155 or 196</td>
</tr>
<tr>
<td>ecp</td>
<td>Elliptic Curve (char. P; ANSI X9.62/63, IEEE P1363)</td>
<td>160 or 192</td>
</tr>
<tr>
<td>rsa</td>
<td>RSA (ANSI X9.31, PKCS#1)</td>
<td>1024, 2048, 512 or 768</td>
</tr>
</tbody>
</table>
Message Digest

Hashing is the process of obtaining a relatively short message digest, or “fingerprint,” from a typically large data stream for use in message authentication or digital signatures. SecretAgent 5 primarily uses two message digest functions: SHA-1 (the NIST Secure Hash Algorithm, FIPS 180-1) and MD5 (RFC1321). MD2 (RFC1319) may occasionally be used to validate the root certificate issued by certain certificate authorities.

Validity Period and Key Usage Settings

The Set Validity Period and Extensions dialog box allows you to set the effective dates, define the key usage, and set the criticality option in the certificate.

Not Before  Set the effective start date for the certificate. Use the drop-down calendar graphic to select a date from a calendar control.

Not After  Set the effective end date for the certificate. Use the drop-down calendar graphic to select a date from a calendar control.
**Key Usage**
Select one of the three key usage extensions: Encrypting only, Signing only, or Encrypting, signing or both.

**Criticality**
Select non-critical or critical to specify how other applications should process the Key Usage extension in the certificate. (SecretAgent 5 always honors the Key Usage extension regardless of the criticality flag, but other applications may ignore this extension if it is flagged non-critical.)

**Specifying a Password**
The Enter Your Password dialog box allows you to specify the password that will be used to protect your private key.

![Enter Your Password Dialog Box](image)

**Enter Password**
Type a word or phrase (minimum 8 characters; maximum 40 characters) that you will use as your password. Passwords are case sensitive. Be sure to choose a strong password; do not choose a single dictionary word.

If you would like SecretAgent to suggest a strong password, click the **Suggest Password** button.
This dialog generates a random password using the (DES-based) FIPS 181 standard. The spin controls allow you some control over the length of the suggested passphrases and some pronunciation help is provided as a mnemonic aid.

If you are dissatisfied with the suggestion, you may click **Suggest Another** as may times as you like. Click **OK** to accept the current suggestion and copy it back to the Password dialog, or click **Cancel** to return to the Password dialog without it.

**Confirm Password**

Retype your password in the Confirm Password text box when prompted. Passwords are case sensitive and you must type your password exactly the same each time you enter it. (If you accepted the FIPS 181 suggested password, this is a good time to see if you can remember it!)
Storing the Certificate

The Specify Disposition for Certificate/Request dialog box allows you to control how the certificate or certificate request will be handled and stored. Typically, self-signed certificates are simply stored locally, but certificate request must often be emailed to a registration authority or CA.

Select at least one of the following:

- **Store the certificate or request in the active certificate folder**
  The certificate will be stored in the SecretAgent 5 Personal Certificate default folder.

- **Write the certificate or request and private key to the following files**:
  Enter target file names (with path) for the public key certificate/request file and/or the private key file, or use the Select buttons to navigate to the desired folder(s).

- **Send the certificate request embedded in an e-mail message**
  If you check this box, SecretAgent 5 will attempt to mail your certificate request via the default MAPI service provider if one is installed on your system.
CHAPTER 7

Application Integration

SecretAgent 5 integrates with a number of office productivity products running on the Windows 95, 98, 2000, and NT 4.0 operating systems. You may be able to access the security features of SecretAgent while working wholly within your e-mail or office suite application.

For example, if Microsoft Office Suite 95, 97, or 2000 is installed on your system when you install SecretAgent 5, the Setup program will detect the presence of Microsoft Word, Excel, and PowerPoint and integrate itself into their menu systems (either automatically or optionally depending on whether you have chosen the Typical or Custom installation type).

This chapter discusses the integration of SecretAgent with the following applications:

- Microsoft Word (Office 95/97/2000)
- Microsoft Excel (Office 95/97/2000)
- Microsoft PowerPoint (Office 97/2000)

Integration with Third Party Applications

SecretAgent 5 offers seamless integration with several of the applications in Microsoft Office 95, 97 and 2000. The program also works with a wide range of e-mail and office productivity applications that run on Windows operating systems. For current information about SecretAgent 5 and third-party application integration, see the Readme text file included on the CD-ROM and ISC’s website, http://www.infoseccorp.com.
SecretAgent 5 and Microsoft Word

This section describes the processes for encrypting and decrypting Microsoft Word documents.

Encrypting a Word Document

The following procedure assumes that the document you wish to encrypt is currently open in Word and was previously saved (in plaintext format) as filename.doc in some folder on your hard drive. Note that when you encrypt this document using SecretAgent, it will be saved as filename[doc].sa5 in your default ciphertext folder (which is typically [SA5 folder][UserName]Cipher) and, of course, this encrypted copy of the file will bear a SecretAgent 5 icon instead of the usual icon for Microsoft Word documents.

⇒ To encrypt a document from Word:

1. Select File, Save from the File menu in Word to save the document. (You will have to enter a file name if this is the first time you’re saving the document to disk.)

2. Click the SecretAgent icon on the Formatting toolbar or select Tools, SA5 Encrypt… from Word’s Tools menu.
3. If you have more than one personality defined, the Personality Manager dialog box will appear. Select an appropriate entry in the Personalities list and click **Login** to launch SecretAgent 5.

In any case, the Encryption dialog box should appear next:

4. Select one or more names from the Available Certificates list and click **>>** to copy them to the Selected Recipients list.

5. Click **OK** to encrypt and close the Word document. An encrypted copy of your document is placed in your ciphertext folder.
Decryption a Word Document

When you decrypt a (single) Word document using SecretAgent 5, it is saved as `filename.doc` in your default plaintext folder (typically `[SA folder]\[UserName]\Plain`). Of course, its original the Microsoft Word icon is restored.

To decrypt a Word document:

1. Run SecretAgent 5 and select Decrypt on the Tool/Menu bar to display the Select Files to Decrypt dialog box.

2. Select the desired ciphertext archive or type its name in the File name text box. (Note that you can also double-click this file name in Windows Explorer to launch SecretAgent automatically.)

3. Click Open to display the Enter Password dialog box.

4. Type your password in the Password text box and click OK to decrypt the document. The plaintext version will be placed in your default plaintext directory.
5. Before SecretAgent’s Decrypt Progress dialog box closes double click a document name in the lower Plaintext Files panel to open it in Word.

**SecretAgent 5 and Microsoft Excel**

The procedures that follow describe the processes for encrypting and decrypting Excel spreadsheets.

**Encrypting an Excel Spreadsheet**

The following procedure assumes that the spreadsheet you wish to encrypt is currently open in Excel and was previously saved (in plaintext format) as `filename.xls` in some folder on your hard drive. Note that when you encrypt this document using SecretAgent, it will be saved as `filename[xls].sa5` in your default ciphertext folder (which is typically `[SA5 folder]\[UserName]\Cipher`) and, of course, this encrypted copy of the file will bear a SecretAgent 5 icon instead of the usual icon for Microsoft Excel documents.

To encrypt an Excel spreadsheet:

1. Select **File, Save** from the File menu in Excel to save the spreadsheet file. (You will have to enter a file name if this is the first time you’re saving the document to disk.)

2. Select **Tools, SA5 Encrypt...** from Excel’s Tools menu.

3. If you have more than one personality defined, the Personality Manager dialog box will appear. Select an appropriate entry in the Personalities list and click **Login** to launch SecretAgent 5.
In any case, the Encryption dialog box should appear next:

4. Select one or more names from the Available Certificates list and click >> to copy them to the Selected Recipients list.

5. Click OK to encrypt the file and close the Excel file. The encrypted file is placed in your ciphertext folder.
Decrypting an Excel Spreadsheet

When you decrypt a (single) Excel spreadsheet using SecretAgent 5, it is saved as *filename*.xls in your default plaintext folder (typically `[SA folder]\[UserName]\Plain`). Of course, its original the Microsoft Excel icon is restored.

To decrypt an Excel spreadsheet:

1. Run SecretAgent 5 and select Decrypt on the Tool/Menu bar to display the Select Files to Decrypt dialog box.

![Select Files to Decrypt dialog box]

2. Navigate through your folders if necessary and click on the desired ciphertext archive or simply type its name in the File name text box. (Note that you can also simply double click this file in Windows Explorer to launch SecretAgent automatically.)

3. Click Open to display the Enter Password dialog box.

![Enter Password dialog box]

4. Type your password in the Password text box and click OK to decrypt the document. The plaintext version will be placed in your default plaintext directory.
5. Before SecretAgent’s Decrypt Progress dialog box closes, double click a spreadsheet name in the lower Plaintext Files panel to open it in Excel.

SecretAgent 5 and Microsoft PowerPoint

The procedures that follow describe the processes for encrypting and decrypting PowerPoint presentations.

Encrypting a PowerPoint Presentation

The following procedure assumes that the document you wish to encrypt is currently open in PowerPoint and was previously saved (in plaintext format) as filename.ppt in some folder on your hard drive. Note that when you encrypt this document using SecretAgent, it will be saved as filename[.ppt].sa5 in your default ciphertext folder (which is typically [SA5 folder]\[UserName]\Cipher) and, of course, this encrypted copy of the file will bear a SecretAgent 5 icon instead of the usual icon for Microsoft PowerPoint presentations.

To encrypt a PowerPoint presentation:

1. Select File, Save from the File menu in PowerPoint to save the presentation. (You will have to enter a file name if this is the first time you’re saving the document to disk.)

2. Select Tools, SA5 Encrypt... from the Tools menu.

3. If you have more than one personality defined, the Personality Manager dialog box will appear. Select an appropriate entry in the Personalities list and click Login to launch SecretAgent 5.
In any case, the Encryption dialog box should appear next:

4. Select one or more names from the Available Certificates list and click >> to copy them to the Selected Recipients list.

5. Click **OK** to encrypt the file and return to PowerPoint. An encrypted copy of your presentation is placed in your ciphertext folder.
Decrypting a PowerPoint Presentation

When you decrypt a (single) PowerPoint presentation using SecretAgent 5, it is saved as filename.ppt in your default plaintext folder (typically [SA folder]\[UserName]\Plain). Of course, its original the Microsoft PowerPoint icon is restored.

To decrypt a PowerPoint presentation:

1. Run SecretAgent 5 and select Decrypt on the Tool/Menu bar to display the Select Files to Decrypt dialog box.

2. Navigate through your folders if necessary and click on the desired ciphertext archive or simply type its name in the File name text box. (Note that you can also simply double click this file in Windows Explorer to launch SecretAgent automatically.)

3. Click Open to display the Enter Password dialog box.

4. Type your password in the Password text box and click OK to decrypt the document. The plaintext version will be placed in your default plaintext directory.
4. Before SecretAgent’s Decrypt Progress dialog box closes, double click the plaintext file name in the lower Plaintext Files panel to open the presentation in PowerPoint.