

User's Guide

# PolicyAgent and Key Recovery

for SecretAgent® 5.8  
and SpyProof!® 1.2



Information in this document is subject to change without notice and does not represent a commitment on the part of Information Security Corporation. The software described in this document is furnished under a license agreement or nondisclosure agreement.

The software may be used or copied only in accordance with the terms of the agreement. No part of this manual may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose other than the purchaser's personal use without the prior written permission of Information Security Corporation.

SecretAgent software is commercial computer software and, together with any related documentation, is subject to the restrictions on U.S. Government use as set forth below.

**RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software Clause at DFARS 52.227-7013.

“Contractor/manufacturer” is Information Security Corporation, 1141 Lake Cook Road Suite D, Deerfield, IL 60015-9461.

The U.S. International Traffic in Arms Regulations (ITARs) (22 CFR 125.03) prohibits the dissemination of certain types of technical data to foreign nationals.

Protected by U.S. Patents No. 5,274,707 and 5,373,560.

Microsoft, Microsoft Word, Excel, PowerPoint, Exchange, and Outlook are registered trademarks of Microsoft Corporation.

SecretAgent is a registered trademark of Information Security Corporation.

Copyright © 1991-2004 Information Security Corporation. All rights reserved.

Printed in U.S.A., PolicyAgent, first edition (November 2004)

**Information Security Corporation**

1141 Lake Cook Road, Suite D

Deerfield, IL 60015-9461

Product Information: 800-203-5563

Technical Support: 847-405-0757

Internet Support: [tech@infoseccorp.com](mailto:tech@infoseccorp.com)

Document No. ISC-PA-0580-11112004

Printed in the United States

## Table of Contents

<b>Chapter 1: Introduction</b>	<b>4</b>
Using this Guide	4
Conventions Used in this Guide	5
Print Conventions	5
Command Terminology	5
Mouse Conventions	6
System Requirements	6
System Software	6
Hardware Requirements	6
Important Information	7
<b>Chapter 2: PolicyAgent</b>	<b>8</b>
Installing PolicyAgent	8
PolicyAgent Window	12
ISC Products Policy Settings	14
Trust Policy	14
Recovery Agents	16
SecretAgent Security Policy Settings	18
Cryptography	18
Certificate Policy	22
LDAP Queries	27
Audit Policy	28
User Interface	28
Passwords	34
Server Configuration	36
Exclude Folders	37
SpyProof! Security Policy Settings	39
Algorithms	39
Configuration	40
Hot Key	40
Building a PolicyAgent Distribution	43
<b>Chapter 3: Deployment</b>	<b>45</b>
Creating the Installation Package	45
Installing the Installation Package	47
Creating Automatic Update Packages	47
Changing the Policy Signing Certificate	48
<b>Chapter 4: Key Recovery Utility</b>	<b>50</b>
Installing the Key Recovery Utility	50
Configuring the KRU	53
Recovering Messages with the KRU	55

# Chapter 1: Introduction

PolicyAgent and Key Recovery Utility enable strict enforcement of permissions granted to the users of SecretAgent for Windows and SpyProof! These applications are intended for Security Administrators in an organization. With PolicyAgent the administrator can define a security policy that decides which SecretAgent and SpyProof! settings should be allowed to the end user. The Key Recovery Utility (KRU) provides a mechanism for the recovery of encrypted messages when a user's private key is unavailable. Key recovery only recovers the specific session key used to encrypt a particular document and does not recover a user's private key.

PolicyAgent and the Key Recovery Utility are fully compatible with Windows 95, Windows 98, Windows ME, Windows NT 4.0 Workstation and Server operating systems, Windows 2000, and Windows XP.

## Using this Guide

This User's Guide provides information that will assist you in effectively using PolicyAgent and the Key Recovery Utility. It is divided into four chapters:

### *Chapter 1: Introduction*

Provides an overview of the organization and contents of the guide, presents the style conventions used, reviews system requirements, and gives you an overview of the features built in to PolicyAgent and the Key Recovery Utility.

### *Chapter 2: PolicyAgent*

Provides an overview of PolicyAgent, including installation instructions and descriptions of the various options available to the administrator that can be enforced in SecretAgent.

*Chapter 3: Deployment*

Describes the key steps needed to install SecretAgent with PolicyAgent settings enforced.

*Chapter 4: Key Recovery*

Describes the operation of the Key Recovery Utility, showing how to install, configure and use the Key Recovery Utility to recover files encrypted with SecretAgent.

## Conventions Used in this Guide

This User's Guide consistently employs certain formatting and language conventions to assist you in learning how to use PolicyAgent and the Key Recovery Utility.

### Print Conventions

The following conventions are used throughout this guide for screen displays, command entries, and keyboard characters:

- ♦ Window titles, menu names, and dialog names are printed in **bold type** and match those in the application. For example: Click **Profile**.
- ♦ 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 **Profile, Preferences** from the Tool bar,” click the arrow next to the **Profile** button on the toolbar 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 over an object 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.

## System Requirements

### System Software

PolicyAgent and the Key Recovery Utility require a 32-bit Microsoft Windows operating system: Windows 95, 98, ME, NT 4.0 Workstation or Server, Windows XP, or Windows 2000. The corresponding version of SecretAgent must also be installed on the system prior to installation of PolicyAgent.

### Hardware Requirements

PolicyAgent and the Key Recovery Utility operate 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)

## Important Information

Before installing or using PolicyAgent or the Key Recovery Utility 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 8:30 a.m. and 5:00 p.m. Central Time. You may also send email to [tech@infoseccorp.com](mailto:tech@infoseccorp.com) or fax your questions to (847) 405-0506.

For current product information, visit Information Security Corporation's website at: <http://www.infoseccorp.com>.

# Chapter 2: PolicyAgent

PolicyAgent is a utility for security administrators to configure the functionality of SecretAgent on users' systems. PolicyAgent creates files that the administrator should distribute with SecretAgent as described in Chapter 3: *Deployment*.

This chapter covers:

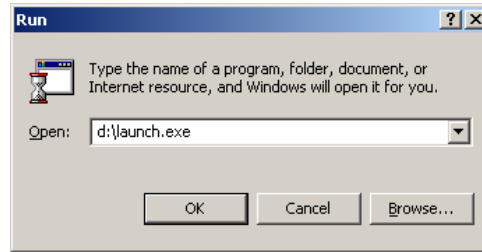
- ◆ Installation of PolicyAgent.
- ◆ Definition and configuration of the options available through the PolicyAgent window.
- ◆ Building a PolicyAgent distribution

## Installing PolicyAgent

PolicyAgent only needs to be installed on an individual system within an organization. Before installing PolicyAgent make sure the corresponding version of SecretAgent is installed on the system. PolicyAgent creates files that should be deployed along with SecretAgent and/or SpyProof! as described in Chapter 3: *Deployment*.

To install PolicyAgent on a Security Administrator's system:

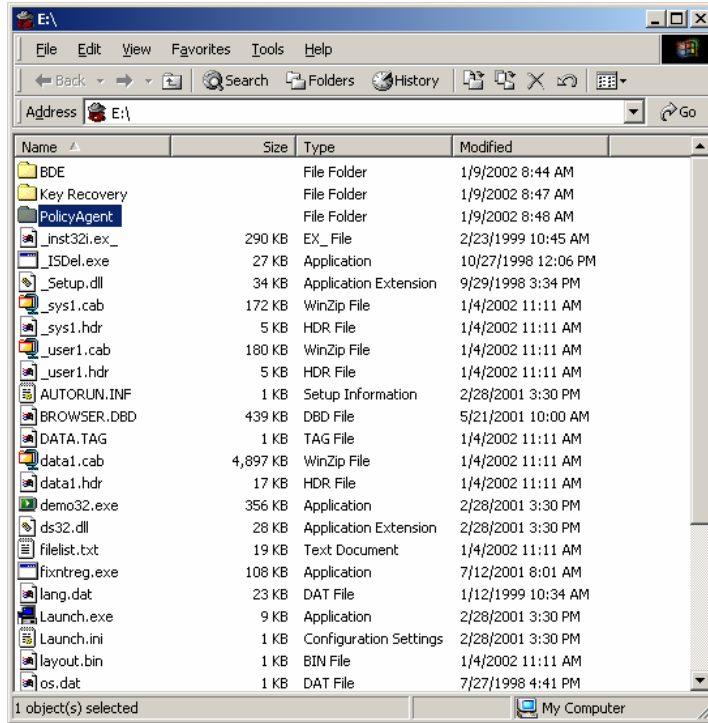
1. Insert the SecretAgent Administrative Utilities CD-ROM into your CD-ROM drive. If your drive supports Auto-Insert Notification and that feature is enabled in Windows, the SecretAgent Setup Program will start automatically. If this occurs, skip the next two steps and proceed to step 4; otherwise continue with step 2.
2. If the SecretAgent Setup Program does not start automatically, select Run from the Windows Start menu.



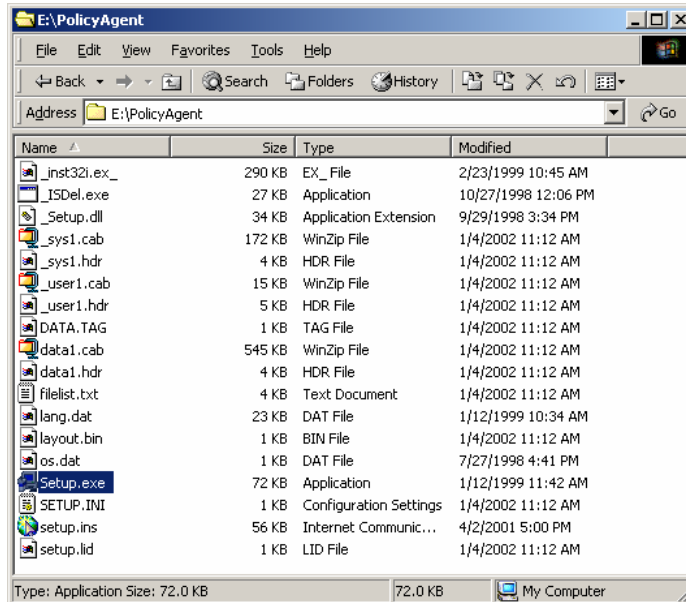
3. Type **D:\Launch** in the Run dialog's Open field and click **OK**. Be sure to substitute an appropriate drive letter if your CD-ROM drive is not D. You will be presented with the SecretAgent Installation Menu:



4. Select **Browse CD Contents**.



5. Double-click on the **PolicyAgent** subdirectory.



6. Double-click on **Setup.exe** to launch the PolicyAgent installation program.

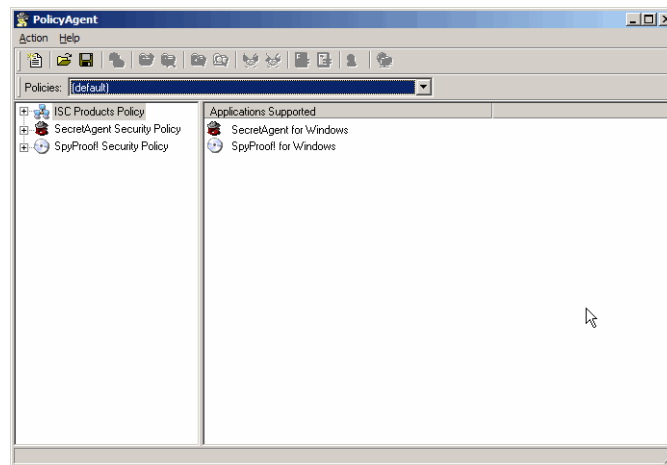


7. Follow the onscreen prompts provided by the installation wizard. PolicyAgent will automatically install in the same directory as SecretAgent.

After you have finished installing PolicyAgent, you can launch PolicyAgent by selecting **Start->Programs->SecretAgent->PolicyAgent.**

## PolicyAgent Window

When you launch PolicyAgent you will be presented with the PolicyAgent window. The PolicyAgent window consists of a tree view on the left containing categories of options you may configure. The right hand pane displays the specific options you may configure in the selected category. To configure a specific option, double-click on that option in the right hand pane. You will be presented with a dialog that will allow you to configure that specific option. Currently, policy settings are divided into three categories: those policies that affect both SecretAgent and SpyProof! (PolicyAgent classifies these under the category **ISC Products Policy**), those policies that affect only SecretAgent, and those policies that affect only SpyProof!



Each policy is governed by a restriction unless noted below:

<b>always enforced</b>	This setting is always enforced by SecretAgent. It typically refers to policies that don't relate to a user option in SecretAgent or SpyProof! For example, <b>Allow private key export</b> is a feature that is either on or off whereas <b>Use base64 encoding</b> is a feature that the user can control and so whether the user can change it or not is up to the security administrator.
<b>user modifiable</b>	This setting is never enforced, but when a new profile or disk is created this will provide the default value for the setting. For example, if you set <b>Use base64 encoding</b> to <b>yes</b> and leave the <b>restriction</b> as <b>user modifiable</b> when the user creates a new SecretAgent profile the profile will have <b>Use base64</b> checked on the <b>Output</b> page of the <b>Profile Preferences</b> dialog for the new profile.
<b>enforced</b>	This setting is enforced. It is like <b>always enforced</b> but

	<p>relates to an option the user usually can control. If your choice is <b>enforced</b> then the user cannot change the option (the particular control is disabled in the application). Continuing the <b>Use base64 encoding</b> example, if you select <b>yes</b> and <b>enforced</b> as the restriction then the user's profile will be set to <b>Use base64</b> and the user will not be able to change the setting. This is useful when you want to ensure that users have a consistent configuration or to make sure users can always decrypt archives they create by forcing users to include themselves on all archives.</p>
n/a	<p>In some cases the particular setting is always user modifiable and the security officer can not enforce the setting on the user but can provide a default value when new profiles or disks are created. For example, <b>Sign by default</b> is marked <b>n/a</b> allowing security officers to either set the <b>Sign plaintext</b> option to yes or no but users can always change this setting (i.e. there is no way to disallow sign and encrypt or enforce encrypt and sign).</p>

The following subsections describe the options available in each of the available categories.

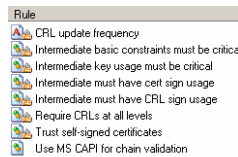
## ISC Products Policy Settings

### Trust Policy

The Trust Policy category contains eight options and two sub categories.



The Trust Policy options deal with certificate validation and trusts. PolicyAgent gives the Security Administrator the ability to automatically distribute CA certificates and the URLs to automatically import and update CRLs to users. To make use of the CA certificate trust and distribution options, the Security Administrator should configure their SecretAgent personal certificate store from within Certificate Explorer so that it contains all applicable CA certificates. To make use of the CRL distribution option, the Security Administrator should import any CRLs to be distributed into Certificate Explorer. Note that only CRLs imported by using a URL can be distributed through PolicyAgent. The Trust Policy options are:











CRL update frequency	Specifies a time interval to have SecretAgent automatically check for updated CRLs. SecretAgent will automatically attempt to download an updated CRL during chain validation if this time period has passed since the last update occurred.
Intermediate basic constraints must be critical	If set to "yes" then only intermediate certificates that have their basic constraints extension marked critical are considered valid.
Intermediate key usage must be critical	If set to "yes" then intermediate certificates' key usage extension must be marked critical.
Intermediate must have cert sign usage	If set to "yes" then intermediate certificates' key usage must include certificate signing.

<a href="#">Intermediate must have CRL Sign usage</a>	If set to “yes” then intermediate certificates’ key usage must include CRL signing when a CRL exists for that authority.
<a href="#">Require CRLs at all levels</a>	If set to “yes” then CRL checking is required so that if the CRL is not valid or if there is no CRL available the end user certificate is not valid.
<a href="#">Trust self-signed certificates</a>	If set to “yes” then users can encrypt with self-signed certificates.
<a href="#">Use MS CAPI for chain validation</a>	If set to “yes” then SecretAgent will default to using Microsoft’s certificate path validation logic rather than its own.

### CA Certificates

The CA Certificates subcategory enables you to select the certificates you wish to distribute and/or trust.

Subject DN	Distribute	Trusted
 CN=C3 ID CAC, OU=PKI, OU=DoD, O=U.S. Government, C=US	no	n/a
 CN=C3 MAIL CAC, OU=PKI, OU=DoD, O=U.S. Government, C=US	no	n/a
 CN=CA1-CP.04.02, OU=Testing, OU=DoD, O=U.S. Government, C=US	no	n/a
 CN=DoD CLASS 3 Root CA DEV, OU=PKI, OU=DoD, O=U.S. Government, ...	no	n/a
 CN=DoD CLASS 3 Root CA, OU=PKI, OU=DoD, O=U.S. Government, C=US	no	n/a
 CN=ISC CA2, OU=Research and Development, O=Information Security Corp...	no	n/a
 CN=ISC Root, L=Deerfield, O=Information Security Corp., ST=IL, C=US	no	n/a
 CN=ISC, OU=R&D, O=ISC, L=Oak Park, ST=Illinois, C=US	no	n/a

PolicyAgent looks in your personal certificate store to locate CA certificates. CA certificates you distribute will automatically be placed in the user’s personal certificate store when SecretAgent is installed on a user’s system. If you mark any CA certificate as trusted or not trusted, all other CA certificates will default to not being trusted unless you configure it otherwise.

### CRL Retrieval

The CRL Retrieval subcategory enables you to publish CRLs you have installed in Certificate Explorer that have update URLs. Only CRLs that have update URLs in Certificate Explorer’s CRL manager will be displayed. The CRL is **not** distributed, but the URL is and the software will automatically retrieve the CRL from the URL as needed.

Subject DN	Published	Modifiable	URL
CN=ISC Root, L=Deerfield, O=Information Security Corp., ST...	no	n/a	http://207.

Any CRL that you mark published in PolicyAgent will be automatically retrieved using the URL the first time SecretAgent is run on a user's system. Marking a CRL as **Modifiable** will allow the end-user to change the URL in Certificate Explorer. If the CRL is not **Modifiable** then users cannot change the URL in Certificate Explorer.

## Recovery Agents

The Recovery Agents category looks in your personal certificate store to locate possible key recovery agents.

Common Name (CN)	Key	Size	SecretAgent Group	SpyProof Group
George W. Bush	DSA	512	Recovery Group 1	Automatic Recipient
Thomas Jefferson	RSA	1024	Automatic Recipient	Automatic Recipient

Using PolicyAgent's Session Key Recovery option, the Security Administrator can specify who will act as Key Recovery Agents to recover encrypted data. More detailed information about the key recovery process can be found in Chapter 4: *Key Recovery Utility*. To make use of the key recovery options, the Security Administrator must first configure their personal certificate store using Certificate Explorer so that it contains the certificates of all people that will be acting as Key Recovery Agents. The following restrictions apply to key recovery agents:

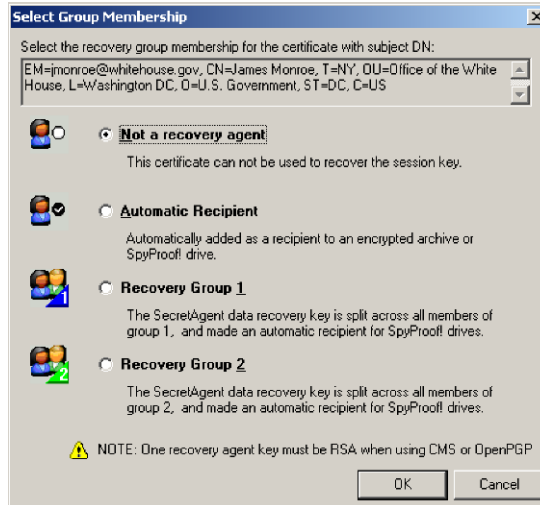
- ◆ Key Recovery Agents in a Key Recovery group must work cooperatively to recover data and all certificates to be placed in an individual Key Recovery Group must have the same key type (DSA/ECDSA) and size.
- ◆ RSA certificates cannot be part of a Recovery Group and can only be marked as Automatic Recipient or Not a Recovery Agent.

- ◆ Only RSA certificates marked as Automatic Recipient will be included when the user creates CMS or OpenPGP archives as these output types do not support DSA, ECDSA, or key recovery groups.
- ◆ SpyProof! only supports Automatic Recipients and so any certificate added as a group recovery agent in SecretAgent is added as an Automatic Recipient in SpyProof!
- ◆ If key recovery is in use and there are no RSA automatic recipients SecretAgent will disable the OpenPGP and CMS output types as they do not support key recovery groups or automatic recipients with key types DSA or ECDSA

The Recovery Agents category enables you to configure your Key Recovery Agents. Certificates can be marked for SecretAgent as members of one of two Recovery Groups, as an Automatic Recipient, or as Not a Recovery Agent. For SpyProof!, all agents that are members of any of the SecretAgent groups or marked as Automatic Recipient are considered Automatic Recipients.

In SecretAgent, those agents marked as Automatic Recipient can recover messages using SecretAgent by themselves without the use of the Key Recovery Utility. Those designated as members of a Recovery Group must work with the other members of their Recovery Group to recover messages using the Key Recovery Utility. In SpyProof! agents can import and mount any disk for which they are a designated agent provided they have the .spd and .spk files for that disk.

By default, all certificates in the database you selected are marked as Not a Recovery Agent. To configure a certificate to act as a Key Recovery Agent, double-click on that certificate. You will see a dialog box similar to the following:



Select the Recovery Setting for this certificate and click **OK**.  
Configure other certificates in your database appropriately.

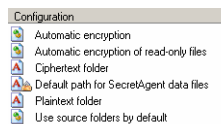
## SecretAgent Security Policy Settings

### Cryptography

The Cryptography category contains six options and three sub categories.



The cryptography options deal with auto-encryption and input and output paths.



The cryptography options are:

Automatic encryption	This option lets you specify values for the auto-encrypt feature of SecretAgent.		
	Setting	Restriction Setting	Description
	yes	user modifiable	New profiles have <b>Encrypt selected folders on exit</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Encrypt selected folders on exit</b> checked by default, and the setting cannot be changed.
	no	user modifiable	New profiles don't have <b>Encrypt selected folders on exit</b> checked by default, but users can enable this option.
	no	enforced	Auto-encryption is disabled.
Automatic encryption of read-only files	Controls the <b>Overwrite read-only files during auto-encrypt/auto-decrypt</b> functionality.		
Ciphertext folder	Enables the specification of a default folder to use for the cipher path folder. This supports environment variable replacement and so can be something like Z:\%USERNAME%\cipher.		
Default path for SceretAgent data files	Enables the specification of the path SecretAgent should use for event logs, profiles, databases, and CRL files. This setting will affect new profile creation but not render existing profiles invalid. This supports environment variable replacement.		
Plaintext folder	Enables the specification of a default folder to use for the plain path folder. This supports environment variable replacement.		
Use source folders by default	Controls the use source folders/use specific folders feature.		
	Setting	Restriction Setting	Description
	yes	user modifiable	New profiles have <b>Always use source folder</b> checked but they can change it.
	yes	enforced	All profiles have <b>Always use source folder</b> checked by default, and the setting cannot be changed.
	no	user modifiable	New profiles have <b>Store output files in these fixed folders</b> checked by default, but users can change this option.
	no	enforced	All profiles have <b>Store output files in these fixed folders</b> checked by default and users cannot select <b>Always use source folder</b> .

*Algorithms*

The Algorithms subcategory configures the available symmetric ciphers available to users of SecretAgent and SpyProof!

Algorithm	Permitted
Cipher: AES-128	yes
Cipher: AES-192	yes
Cipher: AES-256	yes
Cipher: DES3	yes
Cipher: DESX	yes
Cipher: EA2	yes
Default cipher	Cipher: AES-128

Only the Algorithms options set to “yes” will be available to the user. The subcategory Algorithms’ options are:

Cipher: AES-128	When set to “yes” permits users to select AES-128 as their cipher.
Cipher: AES-192	When set to “yes” permits users to select AES-192 as their cipher.
Cipher: AES-256	When set to “yes” permits users to select AES-256 as their cipher.
Cipher: DES3	When set to “yes” permits users to select DES3 as their cipher.
Cipher: DESX	When set to “yes” permits users to select DESX as their cipher.
Cipher: EA2	When set to “yes” permits users to select EA2 as their cipher.
Default cipher	Set the default cipher to use when creating new profiles or disks. If this is set to <b>enforced</b> then users cannot select a different cipher.

*Tokens*

The Tokens subcategory configures which token types a user can use.

Token	Permitted
Default token	Software
FORTEZZA	yes
Microsoft CAPI	yes
Permit future tokens	yes
PKCS #11	yes
Software	yes

Only those tokens set to “yes” can be used by the user. To ensure that users only use PKCS #11 tokens set Software and FORTEZZA

to “no” or specify PKCS #11 as the default token and enforce the setting. The subcategory Tokens’ options are:

Default token	Set the default token to use when creating profiles (this token will be selected when the <b>Select Token</b> page of the <b>New Profile Wizard</b> is displayed). If this setting is enforced then users must use the selected token.
Software	Users may use the built in software module. No hardware token required.
PKCS #11	Users may use PKCS #11 hardware or software tokens.
FORTEZZA	Users may use FORTEZZA cards.
Microsoft CAPI	Users may use the Microsoft CAPI token.
Permit future tokens	Users may use tokens not listed.

### Self-decrypting platforms

The Self-decrypting platforms subcategory determines how SecretAgent treats self-decrypting archives.

Target Platform Options	Permitted
Enable Self-decrypting archives	yes
Output SDA files with ._xe extension	no
Permit future platforms	no
Target: AIX on Power PC	yes
Target: Default	Target: Wi...
Target: HP-LUX	no
Target: IRIX	yes
Target: Linux on Intel	yes
Target: Max OSX Power PC	yes
Target: Solaris on Intel	yes
Target: Solaris on Sparc	no
Target: Tru64	yes
Target: Windows on Intel	yes

The subcategory Self-decrypting platforms’ options are:

Enable Self-decrypting archives	Set to <b>yes</b> to allow users to generate self-decrypting archives. Set to <b>no</b> to prevent users from generating self-decrypting archives.												
Output SDA files with ._xe extension	<p>This option lets you specify the filename extension when users create self-decrypting archives.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>user modifiable</td> <td>New profiles will have ._xe selected as the self-decrypting archive’s output extension, but users can change the setting.</td> </tr> <tr> <td>yes</td> <td>enforced</td> <td>All self-decrypting archives created will end with ._xe.</td> </tr> <tr> <td>no</td> <td>user</td> <td>New profiles will have .exe</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	yes	user modifiable	New profiles will have ._xe selected as the self-decrypting archive’s output extension, but users can change the setting.	yes	enforced	All self-decrypting archives created will end with ._xe.	no	user	New profiles will have .exe
Setting	Restriction Setting	Description											
yes	user modifiable	New profiles will have ._xe selected as the self-decrypting archive’s output extension, but users can change the setting.											
yes	enforced	All self-decrypting archives created will end with ._xe.											
no	user	New profiles will have .exe											

		modifiable	selected as the self-decrypting archive's output extension, but users can change the setting.
	no	enforced	All self-decrypting archives created will end with .exe.
Permit future platforms	Set to <b>yes</b> to allow the user to add and use new self-decrypting archive platforms. Set to <b>no</b> to restrict the user to only those platforms PolicyAgent knows about.		
Target: AIX on Power PC	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: HP-UX	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: IRIX	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: Linux on Intel	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: Solaris on Intel	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: Solaris on SPARC	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: Windows on Intel	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: Mac OSX Power PC	Set to <b>yes</b> to allow users to create self-decrypting archives for this platform. Set to <b>no</b> to prevent users from creating self-decrypting archives for this platform.		
Target: Default	Enables the setting of the default self-decrypting archive format. You can use this to easily specify a single output platform (i.e. restrict all users to using Windows self-decrypting archives).		

## Certificate Store

The Certificate Store category contains eighteen options and two sub categories.



The Certificate Store options control features of Certificate Explorer including certificate stores and certificate/request generation.

Field	Value
CA e-mail address	(not set)
CA Internet address/URL	(not set)
Create CAPI Address Book store	no
Create CAPI CA store	no
Create CAPI My store	no
Create CAPI Root store	no
Default key types/sizes	rsa-1024
Display import certificate warnings	yes
Generate keys	yes
Generate self-signed certificates	yes
Key usage	Encrypt and sign capable
Local Certificate Database Name	Local Certificates
Message digest	SHA-1
PKCS#10 encoding	Base 64
Prevent personal store setting mo...	no
Retrieve missing CRLs or issuer c...	no
Set key usage as critical	no
Validity period	1 Years

The Certificate Store options are:

CA e-mail address	If an e-mail address is present in this setting, certificate explorer will automatically e-mail certificate requests it generates to this e-mail address.									
CA Internet address/URL	Reserved for future use.									
Create CAPI Address Book store	If set to <b>yes</b> Certificate Explorer will automatically contain a store linking to the Other People or Address Book store in Microsoft CAPI.									
Create CAPI CA store	If set to <b>yes</b> Certificate Explorer will automatically contain a store linking to the CA or Intermediate Certificate Authorities store in Microsoft CAPI.									
Create CAPI My store	If set to <b>yes</b> Certificate Explorer will automatically contain a store linking to the My or Personal store in Microsoft CAPI.									
Create CAPI Root store	If set to <b>yes</b> Certificate Explorer will automatically contain a store linking to the Root or Trusted Root Certificate Authorities store in Microsoft CAPI.									
Default key types/sizes	<p>This option lets you pick a single key type and size that all certificate requests and self-signed certificates will use.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Key Type (say RSA-1024)</td> <td>user modifiable</td> <td>The default key type in the certificate or request wizard will be the one selected (e.g. RSA-1024) but users can pick from available key types (see <b>Public Key Types</b> below).</td> </tr> <tr> <td>Key Type (say RSA-</td> <td>enforced</td> <td>Only keys of the type selected will be generated. Users will</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	Key Type (say RSA-1024)	user modifiable	The default key type in the certificate or request wizard will be the one selected (e.g. RSA-1024) but users can pick from available key types (see <b>Public Key Types</b> below).	Key Type (say RSA-	enforced	Only keys of the type selected will be generated. Users will
Setting	Restriction Setting	Description								
Key Type (say RSA-1024)	user modifiable	The default key type in the certificate or request wizard will be the one selected (e.g. RSA-1024) but users can pick from available key types (see <b>Public Key Types</b> below).								
Key Type (say RSA-	enforced	Only keys of the type selected will be generated. Users will								

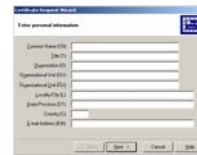
	1024)		see the key selection page but cannot change the value you specify.
Display import certificate warnings	If set to <b>no</b> SecretAgent will not display warnings when importing Root certificates or self-signed certificates.		
Generate keys	Set to <b>yes</b> to allow users to generate self-signed certificates and certificate requests. Set to <b>no</b> to prevent users from generating self-signed certificates or certificate requests. This forces users to use a smart card or import a pre-existing key pair.		
Generate self-signed certificates	Set to <b>yes</b> to enable users to generate self-signed certificates. Set to <b>no</b> to prevent users from generating self-signed certificates. Self-signed certificates enable SecretAgent to be used without a PKI or CA. However, there is no easy way to authenticate a large number of self-signed certificates (for small groups you can exchange self-signed certificates and compare their SHA-1 fingerprint for authentication), as there is no issuing authority. Also you cannot revoke self-signed certificates.		
Key usage	This specifies the key usage to use when creating self-signed certificates.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	Certificates have encrypt privileges	user modifiable	The key usage defaults to Encrypt only.
	Certificates have encrypt privileges	enforced	The key usage defaults to encrypt only and only other <b>enforced</b> options are available.
	Certificates have signing privileges	user modifiable	The key usage defaults to Sign only.
	Certificates have signing privileges	enforced	The key usage defaults to sign only and only other <b>enforced</b> options are available. If this option and the encrypt option above are both enforced then the default is encrypt only and users can create either sign only or encrypt only certificates but not sign and encrypt capable certificates.
	Certificates have both privileges	user modifiable	Key usage defaults to sign and encrypt (a single certificate capable of both signing and encrypting), but other options are available.
	Certificates have both	enforced	The key usage defaults to sign only and only other <b>enforced</b> options are

	privileges		available. If this option and another option above are enforced then this option is the default and users can change to another type.
	Note: This setting only applies to self-signed certificates. If you are going to disable self-signed certificate generation you may ignore this setting.		
Local Certificate Database Name	This allows you to specify a different name for the database that stores the user's private keys and certificate authority certificates.		
Message digest	This specifies the hash function to use when creating either certificates or certificate requests.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	Message digest (say SHA-1)	user modifiable	Sets the default message digest for certificate requests but lets the user pick.
	Message digest (say SHA-1)	enforced	Sets the message digest for certificate requests and prevents user modification of the setting.
	Note: Certain certificate authorities can only support certain combinations of key types and hash algorithms. If you have such a CA this setting enables you to ensure that the correct message digest will be used.		
PKCS #10 encoding	This option determines whether the PKCS #10 requests generated are stored in the database (and if output as files) in binary or text-encoded form.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	PKCS#10 encoding (say base64)	user modifiable	Sets the PKCS#10 encoding for certificate requests but lets the user pick.
	PKCS#10 encoding (say base64)	Enforced	Sets the PKCS#10 encoding for certificate requests and prevents user modification of the setting.
Prevent personal store setting modification	Set to <b>yes</b> to prevent users from moving their personal store from its default location. Set to <b>no</b> to enable users to create and mark any certificate store as their personal store.		
Retrieve missing CRLs or issuer certificates if retrieval information is available	Setting this to <b>yes</b> enables SecretAgent to use CRL distribution points and authority information access certificate extensions to retrieve missing items required for path validation.		

Set key usage as critical	Set the criticality of the key usage extension when the user generates a self-signed certificate.		
	Setting	Restriction Setting	Description
	yes	user modifiable	Key usage will be marked critical by default but the user can uncheck the setting.
	yes	enforced	Key usage will be marked critical.
	no	user modifiable	Key usage will not be marked critical by default but the user can check the setting.
	no	enforced	Key usage will not be marked critical.
Note: Setting this extension to critical means that other programs that do not understand the key usage extension will not be able to use the certificate.			
Validity period	This setting determines how long self-signed certificates are valid. Self-signed certificates will be valid for this many days, months, or years from the day they were generated (if the computer's system clock is correct). If the setting is <b>user modifiable</b> the user is allowed to change this period during certificate creation. If the setting is <b>enforced</b> the user cannot change the setting.		

**RDNs**

The RDNs sub-category pre-configures the relative distinguished names that are placed in all self-signed certificates or certificate requests.



Field	Value	Restrictions
Country	(not set)	user modifiable
Locality/City	(not set)	user modifiable
Organization	(not set)	user modifiable
Organization Unit	(not set)	user modifiable
State/Province	(not set)	user modifiable

The RDNs subcategory options are:

Organization	This is the name of your company
Organization Unit	This is the name of your division
Locality/City	This is the name of your city or township
State/Province	This is the name of your state or province

<b>Country</b>	The country/region field is the two letter ISO 3166 country/region code for your country or region
----------------	--

### Public Key Types

The Public Key Types subcategory lets you specify a subset of available keys types for your user to choose from when generating self-signed certificates and certificate requests.

Algorithm	P...	Restrictions
dsa-1024: DSA parameters, 1024 bits	yes	always enforced
dsa-2048: DSA parameters, 2048 bits	yes	always enforced
dsa-4096: DSA parameters, 4096 bits	yes	always enforced
rsa-1024: RSA parameters, 1024 bits	yes	always enforced
rsa-2048: RSA parameters, 2048 bits	yes	always enforced
rsa-4096: RSA parameters, 4096 bits	yes	always enforced
rsa-8192: RSA parameters, 8192 bits	yes	always enforced
US-B-163: US NIST ECP parameters, B-163	yes	always enforced
US-B-233: US NIST ECP parameters, B-233	yes	always enforced
US-B-283: US NIST ECP parameters, B-283	yes	always enforced
US-B-409: US NIST ECP parameters, B-409	yes	always enforced
US-B-571: US NIST ECP parameters, B-571	yes	always enforced
US-P-192: US NIST ECP parameters, P-192	yes	always enforced
US-P-224: US NIST ECP parameters, P-224	yes	always enforced
US-P-256: US NIST ECP parameters, P-256	yes	always enforced
US-P-384: US NIST ECP parameters, P-384	yes	always enforced
US-P-521: US NIST ECP parameters, P-521	yes	always enforced

For each key type on your system you can specify whether or not it is available for users to generate keys.

### LDAP Queries

Similarly to CRLs, PolicyAgent allows the Security Administrator to automatically distribute LDAP Queries to users.

Description	Published	Modifiable	Server Address
AD Group	no	n/a	192.168.0.40
AD-2	no	n/a	192.168.0.40
ISC Test CA	no	n/a	207.16.209.22
Multi-Cert LDAP	no	n/a	207.16.209.2
US Govt. LDAP	no	n/a	207.16.209.2

To use this option, you will first need to configure any LDAP queries you want to distribute using Certificate Explorer. Any LDAP queries you then mark as published in PolicyAgent will be automatically created on the user's system the first time SecretAgent runs. If the query is marked as enforced then the query will always be added (if it gets deleted for some reason) and the user will not be able to modify the query information. LDAP query

configuration, group support and parameterized LDAP queries are explained in the SecretAgent User's Guide.

## Audit Policy

The Audit Policy category gives the Security Administrator the ability to configure the Event Log page of SecretAgent's Preferences dialog.

Audit Policy	Setting	Restrictions
Decrypt events	yes	user modifiable
Encrypt events	yes	user modifiable
Sign events	yes	user modifiable
Verify events	yes	user modifiable
Zap events	yes	user modifiable

The PolicyAgent Audit Policy options determine which SecretAgent events are included in the event log and whether the user can alter these settings. The Audit Policy options are:

<a href="#">Decrypt events</a>	If set to <b>yes</b> and <b>enforced</b> then all decrypt events will be recorded in the event log. If set to <b>no</b> and <b>enforced</b> then no decrypt events will be recorded. If it is <b>user modifiable</b> then the user can enable/disable logging of this event.
<a href="#">Encrypt events</a>	If set to <b>yes</b> and <b>enforced</b> then all encrypt events will be recorded in the event log. If set to <b>no</b> and <b>enforced</b> then no encrypt events will be recorded. If it is <b>user modifiable</b> then the user can enable/disable logging of this event.
<a href="#">Sign events</a>	If set to <b>yes</b> and <b>enforced</b> then all sign events will be recorded in the event log. If set to <b>no</b> and <b>enforced</b> then no sign events will be recorded. If it is <b>user modifiable</b> then the user can enable/disable logging of this event.
<a href="#">Verify events</a>	If set to <b>yes</b> and <b>enforced</b> then all verify and inspect events will be recorded in the event log. If set to <b>no</b> and <b>enforced</b> then no verify events will be recorded. If it is <b>user modifiable</b> then the user can enable/disable logging of this event.
<a href="#">Zap events</a>	If set to <b>yes</b> and <b>enforced</b> then all zap events will be recorded in the event log. If set to <b>no</b> and <b>enforced</b> then no zap events will be recorded. If it is <b>user modifiable</b> then the user can enable/disable logging of this event.

## User Interface

The User Interface category contains two options and one sub category.

Application	URL
Certificate Explorer	(default: http://www.infosecorp.com/prod...
SecretAgent	(default: http://www.infosecorp.com/prod...

The User Interface category lets you specify where users are sent when using the **Support on web** features in SecretAgent. The User Interface options are:

<a href="#">SecretAgent</a>	The URL where users will be sent when using SecretAgent's Support on Web feature.
<a href="#">Certificate Explorer</a>	The URL where users will be sent when using Certificate Explorer's Support on Web feature.

### Profile Preferences

The Profile Preference subcategory lets you specify settings for SecretAgent's user interface.

Configuration	Setting	Restrictions
Allow E-mailing	no	user modifiable
Allow private key export	yes	always enforced
Allow Zapping	no	user modifiable
Always prompt for file overwrite	no	always enforced
Enable RFC 2440/OpenPGP archives	yes	always enforced
Enable RFC 2633/CMS archives	yes	always enforced
Encrypt e-mail by default	no	user modifiable
Generate enveloped/wrapped signatures	yes	user modifiable
Mail signed archive	no	user modifiable
Originators should be included	yes	user modifiable
Originators should be included for mail	yes	user modifiable
Prompt user before deleting files	yes	user modifiable
Sign by default	no	n/a
Sign e-mail by default	no	user modifiable
Start-up view preference	Explorer View	n/a
Use Base64 encoding	no	user modifiable
Use LZSS compression	no	user modifiable

You can specify either default values or enforced values for the following options:

<a href="#">Allow E-mailing</a>	Control the <b>Mail encrypted archives</b> profile option on the <b>User Interface</b> page.		
	Setting	Restriction Setting	Description
	yes	user modifiable	New profiles have <b>Mail encrypted archives</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Mail encrypted archives</b> checked by default, and the setting cannot be changed.
	no	user modifiable	New profiles don't have <b>Mail encrypted archives</b> checked by default, but users can enable this option.
no	enforced	Users cannot mail encrypted	

			archives from SecretAgent.
Allow private key export	If set to <b>yes</b> then users can export their private key through the export wizard in certificate explorer. If set to <b>no</b> users cannot export their private key.		
Allow Zapping	Controls the <b>Zap source files</b> profile option on the <b>User Interface</b> page.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	New profiles have <b>Zap source files</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Zap source files</b> checked by default, and the setting cannot be changed. Users will be forced to zap the source files when encrypting.
	no	user modifiable	New profiles don't have <b>Zap source files</b> checked by default, but users can enable this option.
	no	enforced	Users can't zap files during the encryption process but can still use the zap features.
Always prompt for file overwrite	If set to <b>yes</b> then the overwrite setting ( <b>Output   Files and Folders</b> ) is set to <b>Prompt</b> and the user cannot change the setting. If set to <b>no</b> the user may change another overwrite setting.		
Enable RFC 2440/OpenPGP archives	If set to <b>yes</b> then the software allows the user to create OpenPGP archives. If set to <b>no</b> the user cannot create OpenPGP archives but they can still decrypt them.		
Enable RFC 3369/CMS archives	If set to <b>yes</b> then the software allows the user to create CMS archives. If set to <b>no</b> the user cannot create CMS archives but they can still decrypt them.		
Encrypt e-mail by default	Controls the <b>Encrypt e-mail messages</b> profile option (on the <b>Plug-ins</b> page).		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	New profiles have <b>Encrypt e-mail messages</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Encrypt e-mail messages</b> checked by default, and the setting cannot be changed.
	no	user modifiable	New profiles don't have <b>Encrypt e-mail messages</b> checked by default, but users can enable this option.
	no	enforced	Users can't select to have all e-mail messages they compose in their e-mail client to be encrypted by default.

Generate enveloped/wrapped signatures	<p>Controls the <b>Signature</b> options on the <b>User Interface</b> page.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>user modifiable</td> <td>New profiles have <b>Enveloped signatures</b> checked by default, but users can change the setting.</td> </tr> <tr> <td>yes</td> <td>enforced</td> <td>All profiles have <b>Enveloped signatures</b> checked by default, and the setting cannot be changed. Users will always create enveloped signatures</td> </tr> <tr> <td>no</td> <td>user modifiable</td> <td>New profiles have <b>Detached signatures</b> checked by default, but users can enable this option.</td> </tr> <tr> <td>no</td> <td>enforced</td> <td>New profiles have <b>Detached signatures</b> checked by default and this setting cannot be changed. Users will always create detached signatures.</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	yes	user modifiable	New profiles have <b>Enveloped signatures</b> checked by default, but users can change the setting.	yes	enforced	All profiles have <b>Enveloped signatures</b> checked by default, and the setting cannot be changed. Users will always create enveloped signatures	no	user modifiable	New profiles have <b>Detached signatures</b> checked by default, but users can enable this option.	no	enforced	New profiles have <b>Detached signatures</b> checked by default and this setting cannot be changed. Users will always create detached signatures.
Setting	Restriction Setting	Description														
yes	user modifiable	New profiles have <b>Enveloped signatures</b> checked by default, but users can change the setting.														
yes	enforced	All profiles have <b>Enveloped signatures</b> checked by default, and the setting cannot be changed. Users will always create enveloped signatures														
no	user modifiable	New profiles have <b>Detached signatures</b> checked by default, but users can enable this option.														
no	enforced	New profiles have <b>Detached signatures</b> checked by default and this setting cannot be changed. Users will always create detached signatures.														
Mail signed archive	<p>Control the <b>Mail signed archives</b> profile option on the <b>User Interface</b> page.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>user modifiable</td> <td>New profiles have <b>Mail signed archives</b> checked by default, but users can change the setting.</td> </tr> <tr> <td>yes</td> <td>enforced</td> <td>All profiles have <b>Mail signed archives</b> checked by default, and the setting cannot be changed.</td> </tr> <tr> <td>no</td> <td>user modifiable</td> <td>New profiles don't have <b>Mail signed archives</b> checked by default, but users can enable this option.</td> </tr> <tr> <td>no</td> <td>enforced</td> <td>Users cannot mail signed archives from SecretAgent.</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	yes	user modifiable	New profiles have <b>Mail signed archives</b> checked by default, but users can change the setting.	yes	enforced	All profiles have <b>Mail signed archives</b> checked by default, and the setting cannot be changed.	no	user modifiable	New profiles don't have <b>Mail signed archives</b> checked by default, but users can enable this option.	no	enforced	Users cannot mail signed archives from SecretAgent.
Setting	Restriction Setting	Description														
yes	user modifiable	New profiles have <b>Mail signed archives</b> checked by default, but users can change the setting.														
yes	enforced	All profiles have <b>Mail signed archives</b> checked by default, and the setting cannot be changed.														
no	user modifiable	New profiles don't have <b>Mail signed archives</b> checked by default, but users can enable this option.														
no	enforced	Users cannot mail signed archives from SecretAgent.														
Originators should be included	<p>Controls the <b>Include me as a recipient</b> profile option on the <b>User Interface</b> page.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>user modifiable</td> <td>New profiles have <b>Include me as a recipient</b> checked by default, but users can change the setting.</td> </tr> <tr> <td>yes</td> <td>enforced</td> <td>All profiles have <b>Include me as a recipient</b> checked by default, and the setting cannot be changed. The profile's associated encrypting certificate will be included on all</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	yes	user modifiable	New profiles have <b>Include me as a recipient</b> checked by default, but users can change the setting.	yes	enforced	All profiles have <b>Include me as a recipient</b> checked by default, and the setting cannot be changed. The profile's associated encrypting certificate will be included on all						
Setting	Restriction Setting	Description														
yes	user modifiable	New profiles have <b>Include me as a recipient</b> checked by default, but users can change the setting.														
yes	enforced	All profiles have <b>Include me as a recipient</b> checked by default, and the setting cannot be changed. The profile's associated encrypting certificate will be included on all														

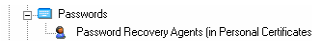
			archives created.
	no	user modifiable	New profiles don't have <b>Include me as a recipient</b> checked by default, but users can enable this option.
	no	enforced	Users cannot use the <b>Include me</b> feature to add themselves as recipients to archives. They must explicitly add themselves as they do other users.
Originators should be included for mail	Controls the <b>Include me as a recipient for encrypted e-mail</b> profile option on the <b>Plug-ins</b> page.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	New profiles have <b>Include me as a recipient for encrypted e-mail</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Include me as a recipient for encrypted e-mail</b> checked by default, and the setting cannot be changed. The profile's associated encrypting certificate will be included on all encrypted e-mail they send.
	no	user modifiable	New profiles don't have <b>Include me as a recipient for encrypted e-mail</b> checked by default, but users can enable this option.
	no	enforced	Users cannot use the <b>Include me as a recipient for encrypted e-mail</b> feature to add themselves as recipients to archives. They must explicitly add themselves as they do other users (yes they must put their e-mail address in the TO or BCC field).
Prompt user before deleting files	Controls the advanced user preferences <b>Prompt before deleting ciphertext or zapping plaintext</b> option.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	New profiles have <b>Prompt before deleting ciphertext or zapping plaintext</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Prompt before deleting ciphertext or zapping plaintext</b> checked by default, and the setting cannot be changed.
	no	user modifiable	New profiles don't have <b>Prompt before deleting ciphertext or zapping plaintext</b> checked by default, but users can enable this

			option.
	no	enforced	Users will not be prompted prior to zapping or deleting files.
<a href="#">Sign by default</a>	Controls the <b>Sign plaintext</b> profile option (on the <b>User Interface</b> page). This option is always user modifiable. If set to <b>yes</b> then new profiles will have the <b>Sign plaintext</b> option checked. If set to <b>no</b> then new profiles will not have the <b>Sign plaintext</b> option checked.		
<a href="#">Sign e-mail by default</a>	Controls the <b>Sign e-mail messages</b> profile option (on the <b>Plugins</b> page).		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	New profiles have <b>Sign e-mail messages</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Sign e-mail messages</b> checked by default, and the setting cannot be changed.
	no	user modifiable	New profiles don't have <b>Sign e-mail messages</b> checked by default, but users can enable this option.
	no	enforced	Users can't select to have all e-mail messages they compose in their e-mail client to be signed by default.
<a href="#">Use base64 encoding</a>	Controls the <b>Use base64</b> option on the <b>Output</b> page of the profile options dialog.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	New profiles have <b>Use base64</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Use base64</b> checked by default, and the setting cannot be changed. All output will be base64 encoded.
	no	user modifiable	New profiles don't have <b>Use base64</b> checked by default, but users can enable this option.
	no	enforced	Users can't select to output files base64 encoded.
<a href="#">Use LZSS compression</a>	Controls the <b>Use compression</b> option on the <b>Output</b> page of the profile options dialog.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user	New profiles have <b>Use</b>

		modifiable	<b>compression</b> checked by default, but users can change the setting.
	yes	enforced	All profiles have <b>Use compression</b> checked by default, and the setting cannot be changed. All files will be compressed prior to encryption or enveloped signing.
	no	user modifiable	New profiles don't have <b>Use compression</b> checked by default, but users can enable this option.
	no	enforced	Users can't select to use compression.

## Passwords

The Passwords section lets you specify how SecretAgent manages passwords. It has one sub item that allows you to specify one or more password recovery agents.



The Passwords category lets you set password usage, minimum lengths, quality requirements, expiration, recovery, and caching options.

Configuration	Setting	Restrictions	
Change password warning	(not set)	always enforced	⌵
Default password cache time	5	user modifiable	⌵
Display random number of asterisks	no	always enforced	⌵
Enable simple user password recovery	no	always enforced	⌵
Minimum private key password length	1	always enforced	⌵
Minimum self-decrypting password length	1	always enforced	⌵
Password expiration period	(not set)	always enforced	⌵
Require letters	no	always enforced	⌵
Require numbers	no	always enforced	⌵
Require punctuation	no	always enforced	⌵
Require special characters	no	always enforced	⌵
Single sign-on/permanent password caching	no	user modifiable	⌵
Timed Password Caching	no	user modifiable	⌵
Unique password interval	0	always enforced	⌵

The Passwords options are:

<a href="#">Change password warning</a>	Allows you to specify the number of days before a user's password expires that the user begins receiving warnings.
<a href="#">Default password cache time</a>	Allows you to specify the default password timed password caching value. If you enforced the value the user cannot change the timeout period.
<a href="#">Display</a>	Setting this to <b>yes</b> will cause the password dialogs to display more

random number of asterisks	characters than the user is typing.															
Enable simple user password recovery	Setting to <b>yes</b> will enable user-based password recovery. The user will be prompted when setting or changing their master password to enter a question and answer it. The question will be stored in the registry along with their encrypted master password. When the user clicks the recover button they are presented the question and if they answer correctly their master password will be displayed for them. This simply acts as a secondary password on the private keys and should be treated as such. However it does not obey any of the password requirements.															
Minimum private key password length	Specify the minimum length of the private key password when a user changes their password.															
Minimum self-decrypting password length	Specify the minimum length of the password for self-decrypting archives.															
Password expiration period	Set the number of days after which the user must change their password in order to use the software.															
Require letters	New passwords (for both private keys and self-decrypting archives) must contain letters.															
Require numbers	New passwords (for both private keys and self-decrypting archives) must contain numbers.															
Require punctuation	New passwords (for both private keys and self-decrypting archives) must contain punctuation characters.															
Require special characters	New passwords (for both private keys and self-decrypting archives) must contain special characters.															
Single sign-on/permanent password caching	<p>Controls the <b>Cache passwords permanently</b> option on the <b>Passwords</b> page of the profile options dialog.</p> <table border="1"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Yes</td> <td>user modifiable</td> <td>New profiles have <b>Cache passwords permanently</b> selected.</td> </tr> <tr> <td>Yes</td> <td>enforced</td> <td>All profiles have <b>Cache passwords permanently</b> selected, and the setting cannot be changed.</td> </tr> <tr> <td>No</td> <td>user modifiable</td> <td>New profiles have either timed password caching or <b>Always prompt me for my password</b> selected, but users can change the setting.</td> </tr> <tr> <td>No</td> <td>enforced</td> <td>Users cannot select <b>Cache passwords permanently</b>.</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	Yes	user modifiable	New profiles have <b>Cache passwords permanently</b> selected.	Yes	enforced	All profiles have <b>Cache passwords permanently</b> selected, and the setting cannot be changed.	No	user modifiable	New profiles have either timed password caching or <b>Always prompt me for my password</b> selected, but users can change the setting.	No	enforced	Users cannot select <b>Cache passwords permanently</b> .
Setting	Restriction Setting	Description														
Yes	user modifiable	New profiles have <b>Cache passwords permanently</b> selected.														
Yes	enforced	All profiles have <b>Cache passwords permanently</b> selected, and the setting cannot be changed.														
No	user modifiable	New profiles have either timed password caching or <b>Always prompt me for my password</b> selected, but users can change the setting.														
No	enforced	Users cannot select <b>Cache passwords permanently</b> .														

Time Password Caching	Controls the <b>Cache passwords for X minutes</b> option on the <b>Passwords</b> page of the profile options dialog.		
	Setting	Restriction Setting	Description
	yes	user modifiable	New profiles have <b>Cache passwords for X minutes</b> selected.
	yes	enforced	All profiles have <b>Cache passwords for X minutes</b> selected, and the setting cannot be changed.
	no	user modifiable	New profiles have either permanent password caching or <b>Always prompt me for my password</b> selected, but users can change the setting.
no	enforced	Users cannot select <b>Cache passwords for X minutes</b> .	
Unique password interval	Specify the number of password changes required before the user can reuse a password.		

**Note:** To disable password caching entirely you must set both **Timed Password Caching** and **Single sign-on/permanent password caching** to **no** and **enforced**.

### Password Recovery Agents

The password recovery agents section allows you to specify one or more certificates that will be used to encrypt the users' passwords.

Common Name (CN)	Key	Size	Group Member
Mikoln Holmes	RSA	1024	no



When a user creates or changes their master password it will be encrypted with these certificates and stored in the registry. When the user clicks the recover button the encrypted file will be e-mailed to the e-mail addresses specified in the recovery agent certificates. These agents can then decrypt the password and inform the user of their password.

## Server Configuration

The server configuration category lets you specify the server address and update period for automatic software and policy updates.

Configuration	Setting	Restrictions
Server address	(not set)	always enforced
Update check duration	(not set)	always enforced

The options are:

<a href="#">Server address</a>	The HTTP address and path to the files needed for updates (policy[bin].sgn, saupd[exe].sgn, and sprfupd[exe].sgn)
<a href="#">Update check duration</a>	Specify how frequently the software should check the server for updates.

**Note:** If you don't specify values for both of these entries SecretAgent and SpyProof! will not automatically download updated policies or software fixes. The update program will run and immediately exit on the end user systems.

## Exclude Folders

The exclude folders category lets you specify one or more fixed folders that cannot be encrypted, auto-encrypted, or zapped using SecretAgent. You may choose to protect just the folder or the entire folder structure.

Folder	Include Subfolders
D:\	no
D:\Documents and Settings\	yes

To add a folder, use the **Add Folder** button on the PolicyAgent toolbar as shown here:



Browse to the folder you want to exclude and select OK. To include subfolders set the **Block subfolders** option to **yes**.

## Advanced PKI

The Advanced PKI section has six options and one sub item.



The advanced PKI section controls how SecretAgent's certificate path validation works. These options are based on NIST PKITS and RFC 3280.

Configuration	Setting	Restrictions
Explicit Policy	(not set)	always enforced
Inhibit Any Policy	(not set)	always enforced
Inhibit Policy Mapping	(not set)	always enforced
OCSP Server	(not set)	always enforced
OCSP Server Cert	(not set)	always enforced
Show Policy Qualifiers	yes	always enforced

The options are:

<a href="#">Explicit Policy</a>	Specify the number of certificates that can be skipped before requiring that the certificates contain a policy extension. Set to -1 to disable, set to 0 to enable immediately, set to X to enable after X certificates.
<a href="#">Inhibit AnyPolicy</a>	Specify the number of certificates that can be skipped before preventing the AnyPolicy policy from being used. Set to -1 to disable, set to 0 to enable immediately, set to X to enable after X certificates.
<a href="#">Inhibit Policy Mapping</a>	Specify the number of certificates that can be skipped before preventing policy mapping extensions from being used. Set to -1 to disable, set to 0 to enable immediately, set to X to enable after X certificates.
<a href="#">OCSP Server</a>	Specify the web address (http://...) of an OCSP server that SecretAgent should use for revocation checking.
<a href="#">OCSP Server Cert</a>	Specify the certificate the OCSP server will use when signing responses.
<a href="#">Show Policy Qualifiers</a>	If set to <b>yes</b> SecretAgent will display User Notices found in the ending policy set.

### Policy OIDs

The Policy OIDs section let you specify an initial policy set.



The initial policy set limits the set of certificates that SecretAgent will consider valid to those that contain at least one of the policy OIDs present in the initial policy set.

## SpyProof! Security Policy Settings

### Algorithms

The Algorithms category configures the available symmetric ciphers available to users of SpyProof! and SecretAgent.

Algorithm	Permitted	Restrictions
Cipher: AES-128	yes	always enforced
Cipher: AES-192	yes	always enforced
Cipher: AES-256	yes	always enforced
Default cipher	Cipher: AES-128	user modifiable

Only the Algorithms options set to “yes” will be available to the user. The category Algorithms’ options are:

Cipher: AES-128	When set to “yes” permits users to select AES-128 as their cipher.
Cipher: AES-192	When set to “yes” permits users to select AES-192 as their cipher.

Cipher: AES-256	When set to "yes" permits users to select AES-256 as their cipher.
Default cipher	Set the default cipher to use when creating new profiles or disks. If this is set to <b>enforced</b> then users cannot select a different cipher.

Note that the ciphers are linked to the SecretAgent Algorithms options described earlier. Thus permitting a cipher in one application will allow it in the other. The default ciphers settings are independent however.

## Configuration

The Configuration category lets you specify SpyProof! credential and configuration options.

Configuration	Permitted	Restrictions	Des
Enable CAPI profiles	yes	always enforced	Allow
Enable 'My Documents' option	yes	always enforced	Allow
Enable Password Based Disks	yes	always enforced	Allow
Encrypt Free Space	yes	user modifiable	Caution



The Configuration options are:

Enable CAPI profiles	If set to "yes" then users have the option of using either a configured SecretAgent profile or certificates stored in their personal CAPI store that have associated private keys for their personal certificate. If set to "no" users can only use configured SecretAgent profiles to access their personal certificate and private key.
Enable 'My Documents' option	If set to "yes" then users have the option of designating a disk they create to act as their 'My Documents' folder. This option is available from the Create Disk dialog. If set to "no" then users cannot specify a disk to act as their 'My Documents' folder from the Create Disk dialog.
Enabled Password Based Disks	Reserved for future use
Encrypt Free Space	Used to preset whether free space on encrypted disks is encrypted or not. Set to <b>yes</b> for greatest security. Set to <b>no</b> to enable SpyProof! disks to be compressed during backups.

## Hot Key

The Hot Key category lets you specify hot key settings for SpyProof!'s silent 'Unmount all' hot key. If the end-user activates

the hot key, all currently mounted disks are unmounted without prompting.

Attribute	Permitted	Restrictions
Allow hot key changes	yes	n/a
Hot key character	Q	user modifiable
Hot key uses alt key	yes	user modifiable
Hot key uses ctrl key	no	user modifiable
Hot key uses shift key	yes	user modifiable

The Hot Key options are:

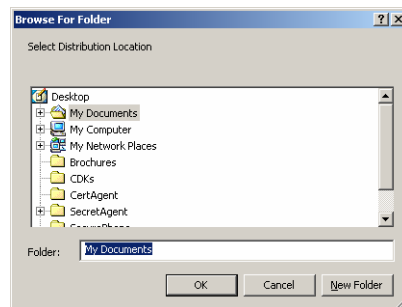
<a href="#">Allow hot key changes</a>	If set to “yes” then users have the option of changing the hot key combination. If set to no, users can only use the hot key combination you specify in the remaining options of this category.															
<a href="#">Hot key character</a>	Specify a character to use as the default hot key character. Only alphabetic characters are allowed. If this is set to <b>enforced</b> then users cannot select a different character.															
<a href="#">Hot key uses alt key</a>	Controls the <b>Alt Key</b> option on the Configure Hot Keys dialog. <table border="1" data-bbox="618 705 1240 1194"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>user modifiable</td> <td>The <b>Alt Key</b> is selected by default to be part of the hot key combination, but users can change the setting.</td> </tr> <tr> <td>yes</td> <td>enforced</td> <td>The <b>Alt Key</b> is selected to be part of the hot key combination and users cannot change the setting.</td> </tr> <tr> <td>no</td> <td>user modifiable</td> <td>The <b>Alt Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.</td> </tr> <tr> <td>no</td> <td>enforced</td> <td>The <b>Alt Key</b> is not selected to be part of the hot key combination, and users cannot change the setting.</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	yes	user modifiable	The <b>Alt Key</b> is selected by default to be part of the hot key combination, but users can change the setting.	yes	enforced	The <b>Alt Key</b> is selected to be part of the hot key combination and users cannot change the setting.	no	user modifiable	The <b>Alt Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.	no	enforced	The <b>Alt Key</b> is not selected to be part of the hot key combination, and users cannot change the setting.
Setting	Restriction Setting	Description														
yes	user modifiable	The <b>Alt Key</b> is selected by default to be part of the hot key combination, but users can change the setting.														
yes	enforced	The <b>Alt Key</b> is selected to be part of the hot key combination and users cannot change the setting.														
no	user modifiable	The <b>Alt Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.														
no	enforced	The <b>Alt Key</b> is not selected to be part of the hot key combination, and users cannot change the setting.														
<a href="#">Hot key uses ctrl key</a>	Controls the <b>Ctrl Key</b> option on the Configure Hot Keys dialog. <table border="1" data-bbox="618 1241 1240 1635"> <thead> <tr> <th>Setting</th> <th>Restriction Setting</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>yes</td> <td>user modifiable</td> <td>The <b>Ctrl Key</b> is selected by default to be part of the hot key combination, but users can change the setting.</td> </tr> <tr> <td>yes</td> <td>enforced</td> <td>The <b>Ctrl Key</b> is selected to be part of the hot key combination and users cannot change the setting.</td> </tr> <tr> <td>no</td> <td>user modifiable</td> <td>The <b>Ctrl Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.</td> </tr> </tbody> </table>	Setting	Restriction Setting	Description	yes	user modifiable	The <b>Ctrl Key</b> is selected by default to be part of the hot key combination, but users can change the setting.	yes	enforced	The <b>Ctrl Key</b> is selected to be part of the hot key combination and users cannot change the setting.	no	user modifiable	The <b>Ctrl Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.			
Setting	Restriction Setting	Description														
yes	user modifiable	The <b>Ctrl Key</b> is selected by default to be part of the hot key combination, but users can change the setting.														
yes	enforced	The <b>Ctrl Key</b> is selected to be part of the hot key combination and users cannot change the setting.														
no	user modifiable	The <b>Ctrl Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.														

	no	enforced	The <b>Ctrl Key</b> is not selected to be part of the hot key combination, and users cannot change the setting.
Hot key uses shift key	Controls the <b>Shift Key</b> option on the Configure Hot Keys dialog.		
	<b>Setting</b>	<b>Restriction Setting</b>	<b>Description</b>
	yes	user modifiable	The <b>Shift Key</b> is selected by default to be part of the hot key combination, but users can change the setting.
	yes	enforced	The <b>Shift Key</b> is selected to be part of the hot key combination and users cannot change the setting.
	no	user modifiable	The <b>Shift Key</b> is not selected by default to be part of the hot key combination, but users can change the setting.
	no	enforced	The <b>Shift Key</b> is not selected to be part of the hot key combination, and users cannot change the setting.

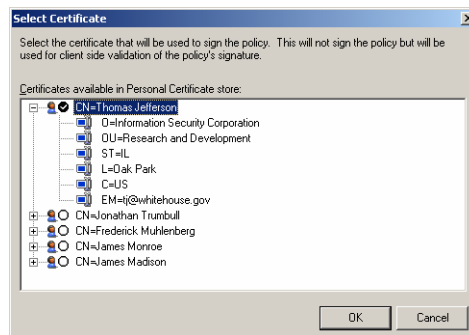
## Building a PolicyAgent Distribution

PolicyAgent supports multiple policies and automatically remembers any changes you make to a particular policy. To create a new policy click **New Policy** on the toolbar or from the menu select **Action->New Policy**. You will be prompted to give the policy a name. Next, configure the policy as desired. Once you are satisfied with a policy you may build a distribution by performing the following series of steps:

1. From the Main Window choose **Action->Build Distribution**. You will be presented with the **Browse for Folder** dialog.



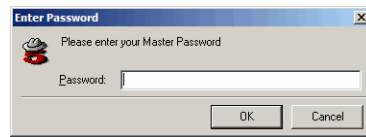
2. Select a location to store your policy files and click **OK**. You will then see the **Select Certificate** dialog.



3. Select the certificate you want to use to sign the policy. Remember the certificate you select. Click **OK**. You will be returned to the Main Window. The following table shows the files created.

<a href="#">policy.bin</a>	This file contains the policy settings. This file will need to be signed using SecretAgent before distribution.
<a href="#">policy.inf</a>	This file contains registry information that SecretAgent and/or SpyProof! will use for verification and updating.

4. Exit PolicyAgent.
5. Start SecretAgent. If not already done, configure your profile so that the profile's signing certificate is the same as the one you selected when building the PolicyAgent distribution.
6. Locate the policy.bin file you created and **Sign** the file. In the Signing Options dialog make sure that **Enveloped Signatures** is enabled.



7. Enter your password and click **OK**. The file policy[bin].sgn will be created in the same directory as the policy.bin file.

You have finished configuring your PolicyAgent settings. You will need both the policy.inf and the policy[bin].sgn files for deployment (the policy.bin file is no longer needed.) Continue to **Chapter 3: Deployment**.

# Chapter 3: Deployment

This chapter provides the basic information you need to deploy SecretAgent and/or SpyProof! when using PolicyAgent.

The procedures in this chapter assume you have completed the creation of a PolicyAgent distribution (see Chapter 2 *PolicyAgent*). First we explain how to create the installation package and then how to install the installation package.

This chapter covers:

- ◆ Creating the Installation Package
- ◆ Installing the Installation Package
- ◆ Creating Automatic Update Packages

## Creating the Installation Package

To begin creating the installation package you will need your SecretAgent and/or SpyProof! CD and the files you created with PolicyAgent. You will also need some means to access these files so that they can be run on the end-user's system.

⇒ **To create the installation package:**

1. Install the SecretAgent or SpyProof! CD in your CD-ROM drive.
2. If installing SecretAgent, if the launch menu appears click Exit.
3. Open Windows Explorer and navigate so that the contents of the CD are visible.
4. Select all individual files in this directory and any subdirectories.
5. Copy these files to a location where a Systems Administrator can access them from users' systems.

6. Next locate the PolicyAgent distribution files (policy.inf and policy[bin].sgn.) Copy these file(s) to the same location you placed the SecretAgent or SpyProof! installation files.
7. After you have copied the necessary files your installation directory should appear similar to the following figure: (Note the location of the policy[bin].sgn and policy.inf files. They must be in the same directory as the setup program to take effect when Setup is run.)

Name	Size	Type	Modified
BDE		File Folder	3/12/2003 9:57 AM
_INST321.EX_	292 KB	EX_File	10/2/1998 7:15 PM
_JSDel.exe	27 KB	Application	10/2/1998 7:06 PM
_Setup.dll	34 KB	Application Extension	9/29/1998 5:34 PM
_sys1.cab	178 KB	WinZip File	3/10/2003 9:20 AM
_sys1.hdr	5 KB	InstallShield Media ...	3/10/2003 9:20 AM
_user1.cab	175 KB	WinZip File	3/10/2003 9:20 AM
_user1.hdr	5 KB	InstallShield Media ...	3/10/2003 9:20 AM
AUTORUN.INF	1 KB	Setup Information	1/16/2003 10:36 AM
BROWSER.DBD	353 KB	DBD File	1/16/2003 10:36 AM
DATA.TAG	1 KB	TAG File	3/10/2003 9:20 AM
data1.cab	8,170 KB	WinZip File	3/10/2003 9:20 AM
data1.hdr	18 KB	InstallShield Media ...	3/10/2003 9:20 AM
demo32.exe	356 KB	Application	1/16/2003 10:36 AM
ds32.dll	28 KB	Application Extension	1/16/2003 10:36 AM
filelst.txt	21 KB	Text Document	3/10/2003 9:20 AM
fixntreg.exe	108 KB	Application	1/16/2003 10:36 AM
lang.dat	5 KB	DAT File	9/18/1998 3:12 PM
Launch.exe	9 KB	Application	1/16/2003 10:36 AM
Launch.ini	1 KB	Configuration Settings	1/16/2003 10:36 AM
layout.bin	1 KB	BITN File	3/10/2003 9:20 AM
os.dat	1 KB	DAT File	7/27/1998 6:41 PM
pkcs11tok.dll	1,306 KB	Application Extension	3/8/2003 8:12 AM
policy.inf	1 KB	Setup Information	3/12/2003 9:19 AM
policy[bin].sgn	3 KB	SecretAgent Signat...	3/12/2003 9:49 AM
ReadMe.txt	24 KB	Text Document	3/10/2003 9:20 AM
sa5.ico	1 KB	Icon	1/16/2003 10:36 AM
SAS60Manual.pdf	5,453 KB	Adobe Acrobat Doc...	1/16/2003 10:36 AM
setup.bmp	148 KB	Bitmap Image	1/16/2003 10:36 AM
Setup.exe	70 KB	Application	10/2/1998 7:04 PM
SETUP.INI	1 KB	Configuration Settings	3/10/2003 9:20 AM
setup.ins	70 KB	Internet Communic...	3/5/2003 2:18 PM
setup.lid	1 KB	LID File	3/10/2003 9:20 AM

You now have all the files needed to properly install SecretAgent or SpyProof! with PolicyAgent settings enforced.

## Installing the Installation Package

This section explains how to use the SecretAgent and SpyProof! Setup Programs to load SecretAgent or SpyProof! with PolicyAgent settings on to a stand-alone computer.

⇒ **To install SecretAgent or SpyProof!:**

1. Logged into the user's system as someone with installation rights, run Setup.exe from the installation directory you created in the previous section.



2. Follow the onscreen prompts provided by the installation wizard. The PolicyAgent settings will be automatically configured during the installation process. After installation, you may need to restart your machine. The installation wizard will notify you if it is necessary to restart your system. The end user should now be able to start using SecretAgent or SpyProof! with all PolicyAgent settings in place.

## Creating Automatic Update Packages

PolicyAgent works with SecretAgent and SpyProof! to enable you to automatically update both the policy and the software itself. The policy files generated (policy.inf and policy[bin].sgn) above can be placed on to a HTTP (web) server and, if configured properly, SecretAgent and SpyProof! will download the updated policy and install it after verifying its signature.

To specify that you want to support automated software and policy updates you must provide a **Server address** (and optional path, e.g. <http://www.infosecorp.com/saupdates>) and **Update check duration** in the **Server configuration** section of the **SecretAgent Security Policy**. Only SecretAgent will update policies and software.

Once the policy has been generated and signed (with the same certificate you used to sign the policy initially distributed when the application was installed) you simply place the policy[bin].sgn file in the folder on the server specified. All clients will automatically download the new policy according to their existing policy.

**Notes:**

- You can change the server address by specifying a new server address in the policy that the clients will download. Clients will then use the server address in the policy file and then use the address in the policy.inf file distributed with the application as a backup address.
- The certificate you picked as the signing certificate when you created the first policy (the one distributed with the application) must be used to sign all following policies (this will likely change in a future release).
- To distribute software updates simply get the update executable from ISC, sign it with the signing certificate you selected for signing policies and place it on the server. SecretAgent updates must be named **saupd[exe].sgn** and SpyProof! updates must be named **sprfupd[exe].sgn**.

## Changing the Policy Signing Certificate

PolicyAgent, SecretAgent, and SpyProof! rely on digital signatures to ensure that the policy installed is valid. This process works by placing the SHA-1 hash of the certificate selected in PolicyAgent when creating a distribution into the registry on each machine that SecretAgent or SpyProof! is installed. When a policy (or signed software update) is verified the signing certificate is hashed and

compared to the entry in the registry. If they match the signature is valid. Otherwise the signature is not valid and the policy or software update is rejected. Since certificates expire a mechanism enabling the replacement of the “old” certificate with a different certificate has been created. Please follow these steps to effect the change over.

1. Create a policy.
2. Build a distribution and select the **new** certificate as the signing certificate.
3. Sign the policy with the **old** certificate.
4. Distribute the policy via the update process.

When the update program downloads this updated policy it will add the certificate hash of the new certificate to the registry. At this point both the old certificate and the new certificate can be used to sign policy and software updates. If you perform this operation more than once only the last two certificates can be used for validation (i.e. after year three only the certificates from years 2 and 3 can be used to sign policies or software updates).

# Chapter 4: Key Recovery Utility

The Key Recovery Utility (KRU) can be used to recover messages encrypted with SecretAgent. The KRU is intended for recovering messages where your key recovery policy involves Key Recovery Groups. Using the KRU may be necessary if the intended original recipient has lost their private key, has forgotten their private key password, is unavailable to decrypt a necessary file, etc. To properly configure key recovery you must configure PolicyAgent so that key recovery settings are enforced as described in **Chapter 2: PolicyAgent**. Then you must deploy these settings onto the end user's system as described in **Chapter 3: Deployment**. For the key recovery process to work, these necessary settings must be deployed *before* the message to be recovered is encrypted. Once the need to recover a message arises, the Key Recovery Agents (KRAs) as designated when creating the PolicyAgent settings in Chapter 2 should follow the instructions outlined in this chapter to recover the message.

This chapter covers:

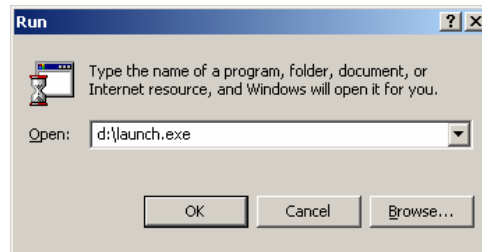
- ◆ Installing the KRU on KRA systems.
- ◆ Configuring the KRU.
- ◆ Recovering messages with the KRU.

## Installing the Key Recovery Utility

The Key Recovery Utility only needs to be installed on the systems of the members of KRA Group 1 and KRA Group 2 as designated in the PolicyAgent settings. Key Recovery Agents designated as Automatic Recipient in PolicyAgent will be able to recover messages through SecretAgent without the use of the KRU.

To install the KRU on a KRA member's system:

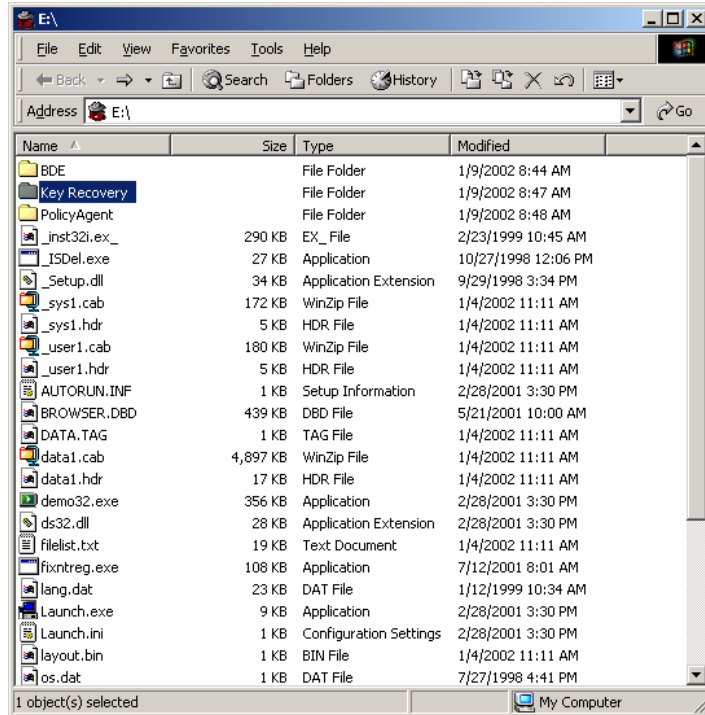
1. Insert the SecretAgent Administrative Utilities CD-ROM into your CD-ROM drive. If your drive supports Auto-Insert Notification and that feature is enabled in Windows, the SecretAgent Setup Program will start automatically. If this occurs, skip the next two steps and proceed to step 4; otherwise continue with step 2.
2. If the SecretAgent Setup Program does not start automatically, select Run from the Windows Start menu.



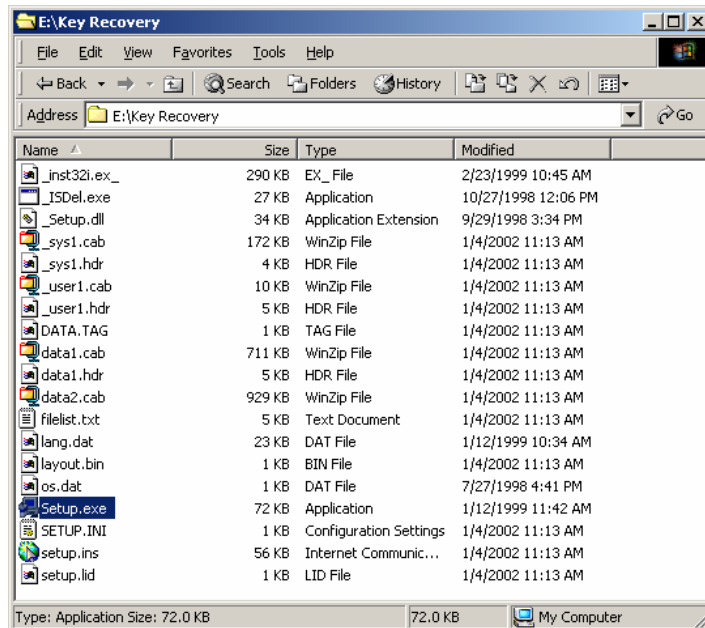
3. Type **D:\Launch** in the Run dialog's Open field and click **OK**. Be sure to substitute an appropriate drive letter if your CD-ROM drive is not D. You will be presented with the SecretAgent Installation Menu:



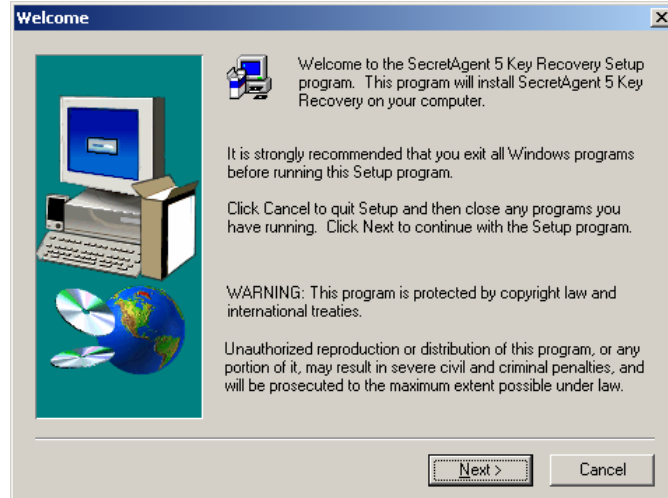
4. Select **Browse CD Contents**.



5. Double-click on the **Key Recovery** subdirectory.



6. Double-click on **Setup.exe** to launch the Key Recovery Utility installation program.



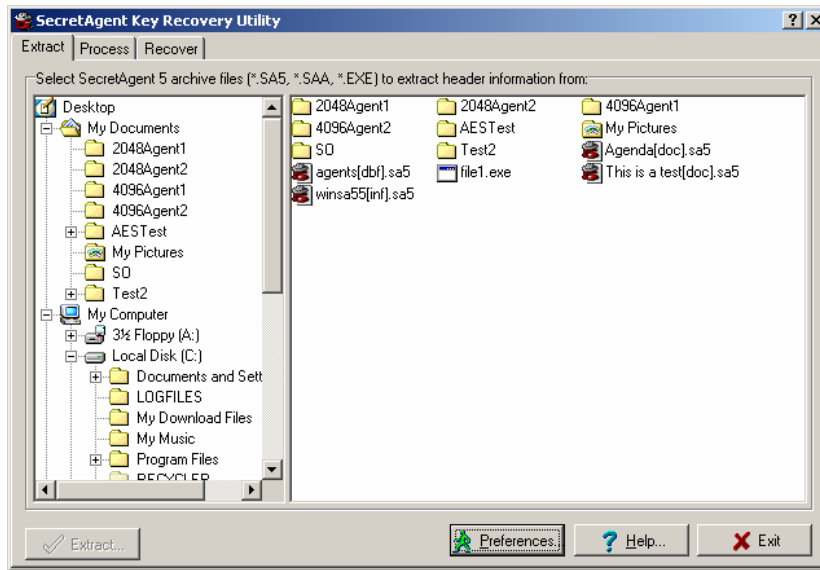
7. Follow the onscreen prompts provided by the installation wizard.

NOTE: The KRU *must* be installed in a different directory than SecretAgent. The default directory provided through the installation wizard reflects this requirement.

After you have finished installing the KRU, you can launch PolicyAgent by selecting **Start->Programs->SecretAgent Key Recovery-> SecretAgent Key Recovery**.

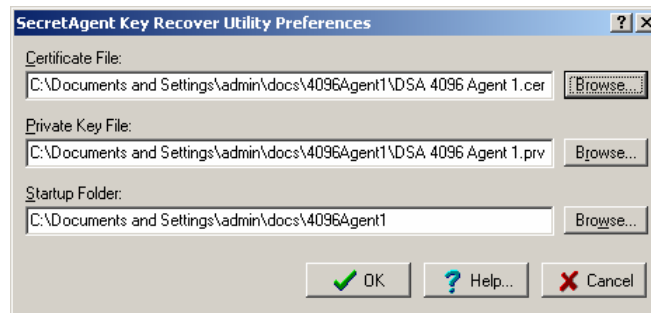
## Configuring the KRU

When you launch the SecretAgent Key Recovery Utility for the first time, you will see the KRU main window. The main windows will be similar to the following figure:



To configure the KRU to recognize your private key do the following:

1. First make sure your certificate and private key have been exported out of Certificate Explorer (see the SecretAgent User's Manual if you need help.)
2. From the KRU main window click the Preferences button. A dialog similar to the following figure will appear.



3. Click the browse buttons to select your certificate file, your private key file, and the folder you would like the KRU to display initially.
4. Click OK to accept these settings.

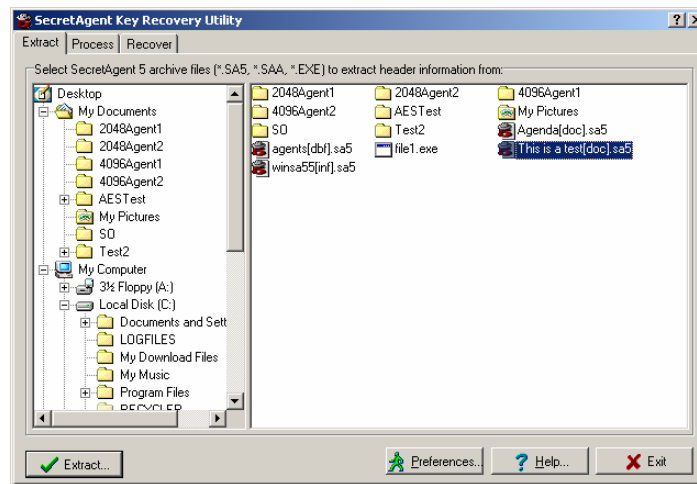
The KRU should now be configured for this Key Recovery Agent. All other key recovery agents should follow the same procedure using their individual certificates and private keys on their respective systems.

## Recovering Messages with the KRU

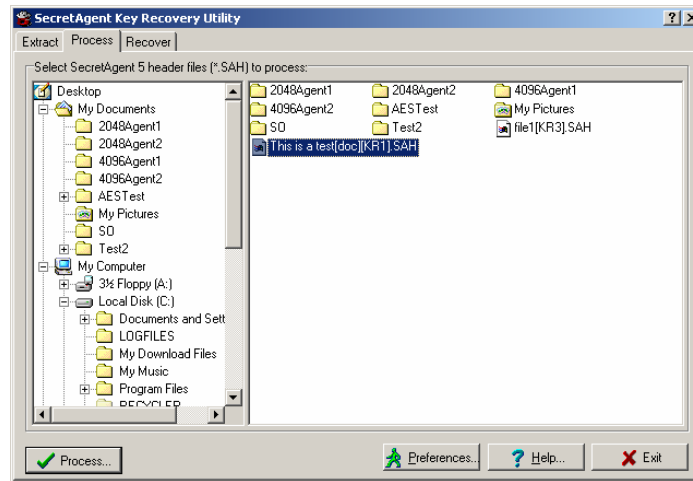
Recovering messages through the KRU requires the cooperation of all KRAs from the same Key Recovery Group. (Note that Key Recovery Agents set as Automatic Recipient in the PolicyAgent settings can recover messages by themselves through SecretAgent without using the KRU.) This section describes how to use the KRU to recover encrypted SecretAgent files.

Once a Key Recovery Agent receives the encrypted SecretAgent files that need to be recovered, the KRA should do the following:

1. Launch the KRU.
2. With the **Extract** tab in the KRU main window active, locate the files to be recovered.



3. Select the files to be recovered from the right hand side.
4. Click the **Extract...** button. For each file selected, this creates a file with a .SAH extension that contains the header information for that particular file.
5. Click **OK**.
6. Click on the **Process** tab and select the .SAH files for the files to be recovered.



7. Click the **Process...** button to process the header files.
8. When prompted for a password, enter your private key password and click **OK**.
9. Click **OK** after the files have been processed.
10. Next, send the .SAH files and the .SAR files to any other member of the Key Recovery Group that has yet to process the files.

If there are more than two members in the Key Recovery Group, all members besides the first and the last should then do the following: (If there are only two members in the Key Recovery Group skip to step 14.)

11. Place the .SAH files and the .SAR files in a single directory.
12. Launch the KRU.
13. Repeat steps 6-10 above.

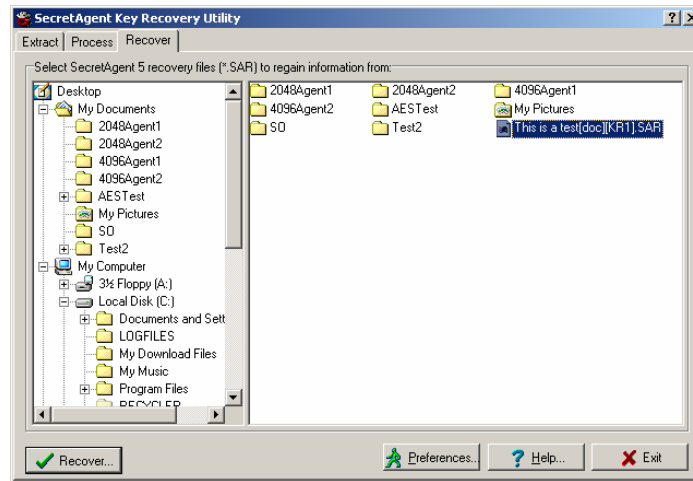
The last KRA in the Key Recovery Group to receive the files should then complete the following steps:

14. Place the .SAH files and the .SAR files in a single directory.
15. Launch the KRU.
16. Repeat steps 6-9 above.

- Next, send the .SAH files and the .SAR files to the first person in the Key Recovery Group (the individual having the original .sa5 file that needs to be recovered).

The first KRA in the Key Recovery Group should then:

- Place the .SAH files and the .SAR files in the directory containing the original encrypted .sa5 files.
- Launch the KRU.
- Click the **Recover** tab.
- Select the .SAR files for the files to be recovered.



- Click the **Recover...** button.

A progress bar will appear. When the recovery is finished, it will show the location of the recovered files. These files are now fully decrypted. The Key Recovery process is complete.