

PolicyAgent™

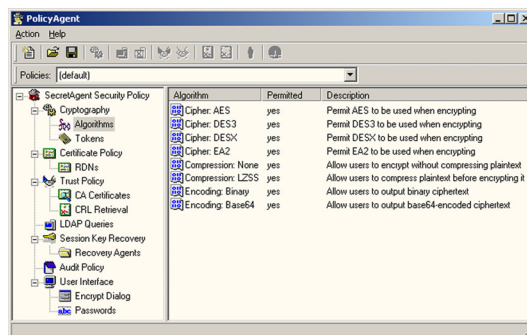
System Requirements

- Microsoft Windows 95, 98, NT 4.0, 2000, ME, or XP
- Intel Pentium II or better CPU
- 32MB RAM
- 15 MB free disk space

Overview

PolicyAgent is a configuration utility for SecretAgent® 5.5 for Windows, ISC's market-leading file encryption software. PolicyAgent supports the corporate security officer in the creation, distribution, and management of security policies for their SA 5.5 users. Providing control over nearly all user-configurable settings, it ensures strict conformance of program usage with the specified security policy.

SecretAgent security policies may include the specification of key recovery agents and trusted root certificates, as well as control the minimum sizes of keys and passwords, enforce CRL usage, and restrict the range of algorithms available to the user. Multiple security policies may be maintained in order to meet differing requirements at the various levels within your organization.



How It Works

PolicyAgent provides an intuitive graphical user interface for editing your security profiles. For each policy, it generates custom installation files that integrate into SA 5.5's standard installation package. After a normal install, these files enforce your security settings and make specified certificates, CRLs, and/or pre-configured LDAP queries available to the user.

Security policies may be updated at any time — simply use your current software distribution mechanisms to install the custom configuration files produced by PolicyAgent.

Policy Enforcement

Once installed by a user with administrative rights, a security policy is protected by strict Windows NT4/2000/XP registry and file system access controls. Your policy is enforced via its control over the behavior of SecretAgent and Certificate Explorer.

Controls and Features

PolicyAgent for SecretAgent 5.5 allows you to:

- Create a key recovery policy by specifying whether key recovery is mandatory and, if so, the individual and/or "shared-secret" groups of key recovery agents (KRAs)
- Specify a list of trusted CAs whose certificates must be used to validate recipient certificates. Trusted root certificates may be included in the SecretAgent software distribution for automatic installation on each user's system
- Enforce CRL checking of all recipient and signing certificates
- Publish update URLs for the CRLs required for your organization
- Distribute pre-configured LDAP queries to all users. Each such query automatically appears in a user's list of available certificate stores
- Permit or disable password caching and control minimum password lengths
- Specify the ciphers, compression options, and output formats that are available to users in the encryption dialog
- Specify exactly which actions should be tracked in each user's event log
- Specify the URLs to be accessed when a user selects the "Support on the Web" help menu item in SecretAgent or Certificate Explorer
- Specify whether users can generate their own self-signed certificates and whether they can use the self-signed certificates of others
- Restrict key type/size choices during key generation to conform to specific CA requirements
- Provide a default e-mail address to which PKCS#10 certificate requests are to be transmitted after key generation
- And much more!



1141 Lake Cook Rd., Suite D
Deerfield, IL 60015

Phone: (847) 405-0500
Fax: (847) 405-0506
E-Mail: sales@infosecorp.com
Web: http://www.infosecorp.com