# CloudProtect: A Developer's Guide and User Manual

Patricia Chin, Mamadou Diallo, Bijit Hore, Sharad Mehrotra

University of California, Irvine

## Abstract

We present a developer's guide, which demonstrates how to incorporate a new service into our cloud encryption middleware, CloudProtect. We also present a user manual to instruct users how to use CloudProtect.

## Developer's Guide

This developer's guide walks through the steps of gathering information and using it to allow incorporate a new web service into CloudProtect.

### I. Object-Oriented Approach

We use objects to describe the general items that the user would want to encrypt in the service. For instance, in GoogleDocs, users would wish to encrypt a document or file and in Google Calendar, an event. Thus, we call the document and event "objects," and the different properties of these items their "attributes."

a. Attribute-value pairs

Each object has a set of attributes, such as ids, dates, and authors. Once these attributes are obtained, the developer can decide which attributes are safe to encrypt and which should be left alone.

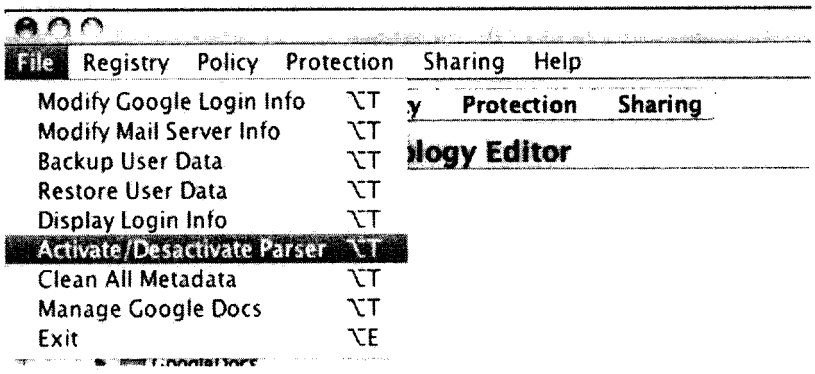
b. Functions

Each service has a series of functions, such as uploading, downloading, and translating. Each function requires certain attributes of the object it is operating on in order to carry out its operation. Thus, attributes serve as both inputs and outputs for functions.

### II. Learning attribute value pairs

a. Activate/deactivate parser on CloudProtect
   The parser assists with finding attribute-value pairs from the desired service.

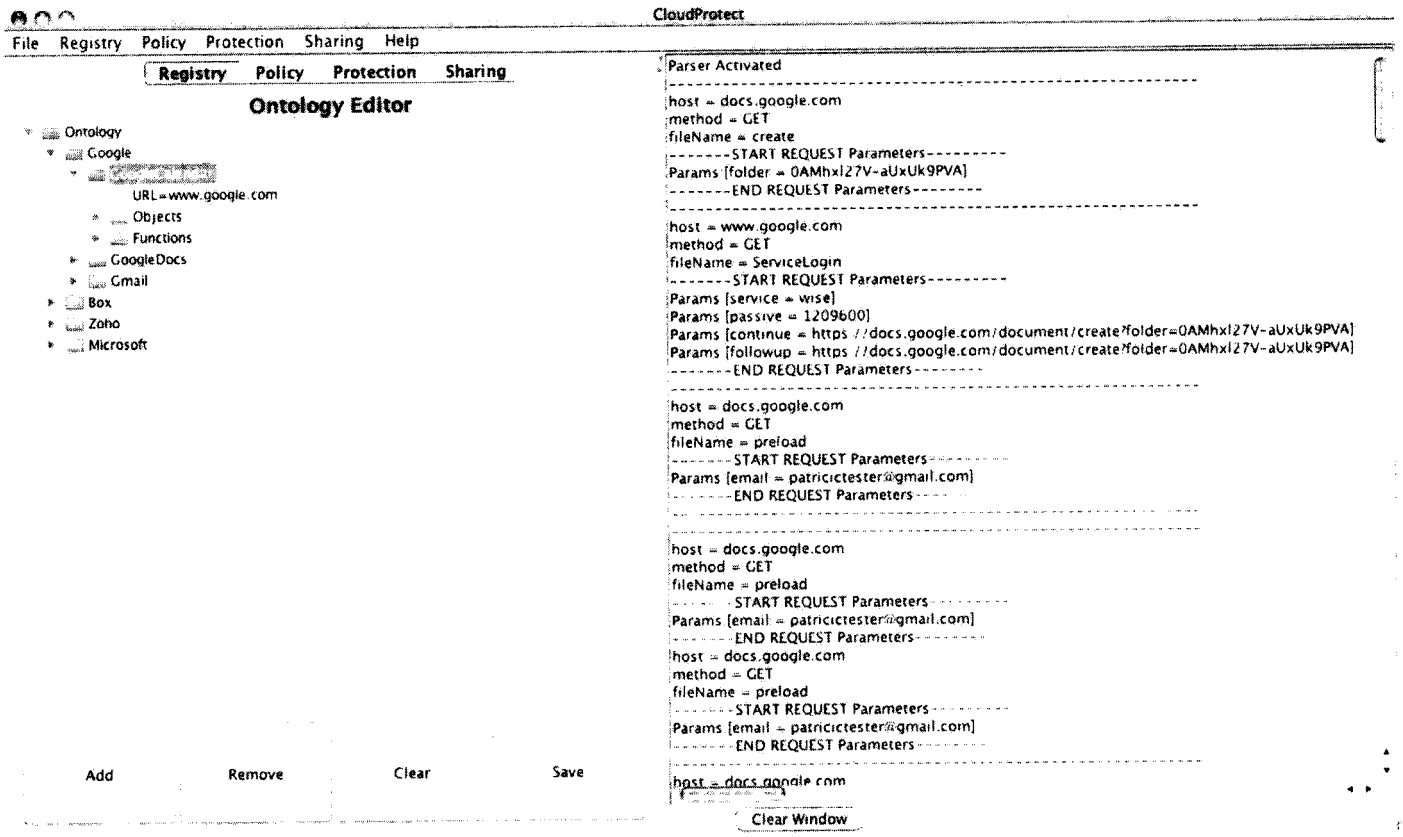
i. **Activating the Parser**
To *activate the parser*, please follow the following steps:
1. Click File → Activate/Deactivate Parser
The right-hand window should now show the words "Parser Deactivated" at the top.




ii. **Deactivating the Parser**
When you want to stop collecting information with the parser, follow the steps below to *deactivate the parser*:
1. Click File → Activate/Deactivate Parser
If any information had been collected in the window, it will be cleared after deactivation. If you want to keep the text shown in the window, please copy and paste the text in a text editor and save it in a separate file. The window should now only have the words "Parser Deactivated" at the top.

**b. Collecting attribute/value pairs**
Make sure that the parser has been activated. After you have verified this, follow the following steps:

i. Go to the website where the desired service is located
ii. Login to the website, if necessary
iii. Perform the function(s) on the website that you would like CloudProtect to handle (e.g. creating a new calendar event, document, etc.)
iv. The parser should now show a series of text, as seen in the figure below:




v. Go through the text and find the --START REQUEST Parameters-- and --END REQUEST Parameters—section that contains data for the functions you tested. In the tested service above, this section has an action, or function, of CREATE, as seen below in the test collected output:

-------START REQUEST Parameters---------
Params:[sf = true]
Params:[output = js]
Params:[action = CREATE]
Params:[add = pchin001@gmail.com,patricictester@gmail.com]
Params:[crm = BUSY]
Params:[icc = DEFAULT]
Params:[sprop = goo.allowModify:false]
Params:[sprop = goo.allowInvitesOther:true]
Params:[sprop = goo.showInvitees:true]
Params:[pprop = eventColor:none]
Params:[text = Misc Testing]
Params:[location = My Room]
Params:[details = CloudProtect Testing for writing up document]
Params:[src = patricictester@gmail.com]
Params:[dates = 20120515T153000/20120515T163000]
Params:[sprop = goo.rtc:0]
Params:[sprop = goo.rtcParam:]
Params:[sprop = goo.rtcDomain:]
Params:[scp = ONE]

```
Params:[nopts = 2]
Params:[nopts = 3]
Params:[nopts = 4]
Params:[secid = _IGUVuu5JC9hHwufYv_B2i5aBK4]
-------END REQUEST Parameters--------
```

vi. From your output, determine which attributes you want to include in your service incorporation for CloudProtect (e.g. add, text, location, details, dates, etc.). Try and distinguish the attribute information from arbitrary HTML data (e.g. scp, nopts, pprop, etc.).

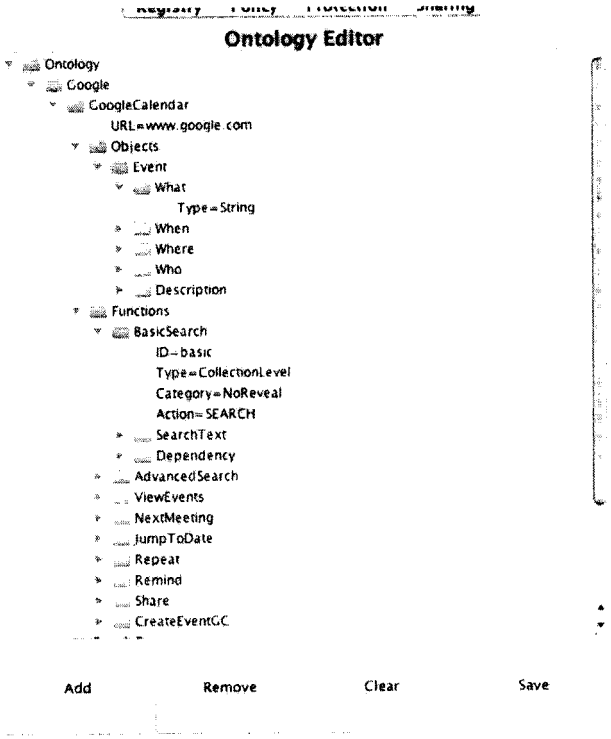
vii. Record these attributes somewhere so you can reference them while registering the web service into CloudProtect

## III. Registering the web service

As mentioned earlier, CloudProtect will use an object-oriented approach to model services. This section will go over the specifics of which folders to create and what type of directory hierarchy to follow in your registration. We will be using GoogleCalendar as an example service to implement.

a. Object-Oriented Model
Each service will have its own object, functions, and attributes. These must be categorized in the ontology editor when registering the service.

b. File Hierarchy



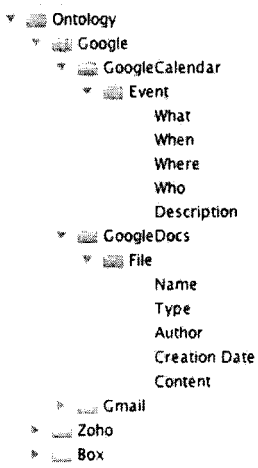
Files need to be organized in a certain fashion. Here are the ways in which files are grouped, in order from outer to inner file directory/file:

- Ontology
  All files and directories go under this folder. In other words, this is the superfolder that contains all the services implanted in CloudProtect.
- Company
  The second-highest priority file directory type is the company file directory. This specifies the company that each service is associated with. For example, Google Calendar is a service provided by the Google company, so there would need to be a "Google" file directory to store the service. This allows users to quickly find services, especially when there are multiple services hosted by the same company.
- Service
  This file directory is for the service that you want to incorporate.
  - URL
    This is where the URL of the service you are using is specified. For instance, the URL for GoogleDocs would be specified like this: "URL=docs.google.com"
  - Objects
    In the example shown in the figure above, the objects are events. Name whichever object type you are using for the service here.
    - Attributes
      These are the properties of the object. For Google Calendars, some of these attributes include what, when, where, who, and description.
  - Functions
    - ID
      Each function requires a unique ID, or name, to identify it.
    - Type
      This can be CollectionLevel or ObjectLevel.
    - Category
      This can be NoReveal, TemporalReveal, or PermanentReveal.
    - Action
      This indicates what type of action this function does. Some examples include SEARCH, CREATE, and NOTIFY. These must be taken from the parser.
    - Dependency
      These list out which attributes the function depends upon.

**c. Different View Modes/Register Menu Items**

There are different ways you may view the ontology/service files. You can toggle the two different views by selecting the Register button on the top menu. You can then choose to open the data ontology or the data and function ontology.

i. Open Data Ontology




As seen above, instead of listing in detail what are the objects and functions associated with a service, this lists out the object name and the attributes associated with it. This can be useful if you want a quick view of what all the attributes are.

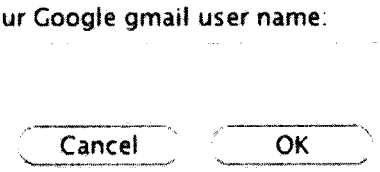
ii. Open Data and Function Ontology
This is simply the first method of laying out the file hierarchy described.

iii. Save Current Ontology
This allows you to save your current ontology/file system. The actual save file can be found in CloudProtect9999/data/download/DataOntology.txt. This data should be backed up so that multiple copies of CloudProtect may be able to access this information.

## User Manual

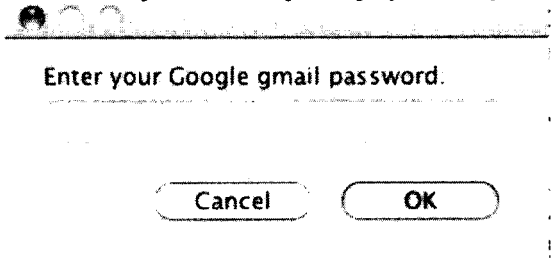
This section will discuss how to do various tasks from a user's point of view.

I. Initial Setup
   a. First, the system will prompt you to provide your Google gmail user name:




e.g. example@gmail.com

b. Next, the system will prompt you for your Google gmail password:

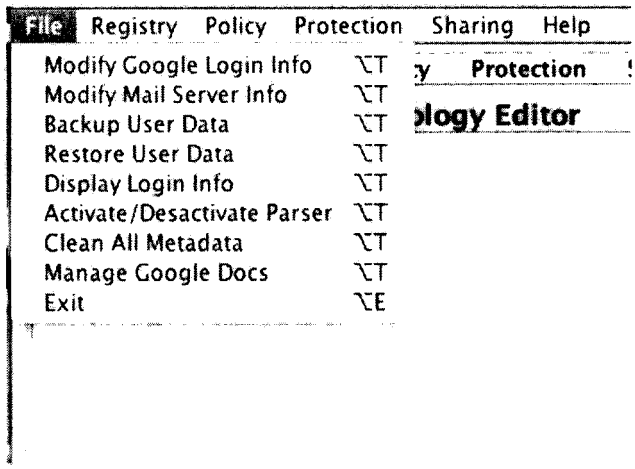



Note: the password will not be hidden.

c. CloudProtect will open up a new window. In the right window pane, there should be some text displaying the information you entered in the first two steps:

```
New Google Login Info
GOOGLE
User Name = patricictester@gmail.com
Password = **********
CloudProtect started.
Listening on port:9999
Configure your browser to use
this server and port as its proxy.
```

II. File...

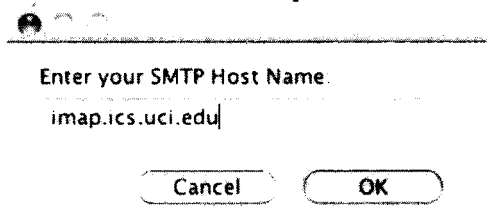



a. Modify Google Login Info
This information is collected during the initial setup.
   i. We are using the API for Google Docs and Calendar, so we need to store the login information (access them directly instead of through the web-based application).
   ii. The login information that needs to be stored includes the username and password.
   iii. Unfortunately, there is no implementation to hide the password as you type it in as of this moment. This change needs to be fixed later.

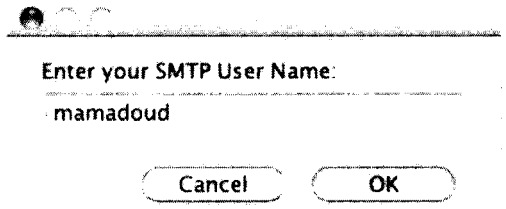
b. Modify Mail Server Info
This information allows you to provide which email provider to send encryption key data from. For example, you can choose to send encryption key emails from gmail, Hotmail, and

other email services. Be sure to check the email service website for information on how to get their SMTP information.

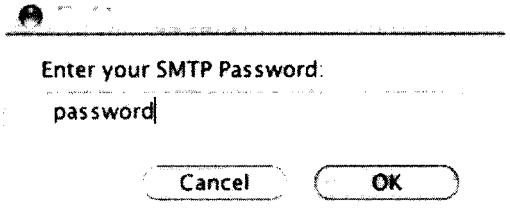
i. CloudProtect requires a user mail server to send encryption key via email to users. This includes sharing of encryption keys between people.
ii. In our sample system, we use the UCI mail server to send the encryption keys. You will need your own SMTP mail server to carry out these operations.
iii. Find out the SMTP host name of one of your email providers. For the UCI ICS email, this host name is "imap.ics.uci.edu";



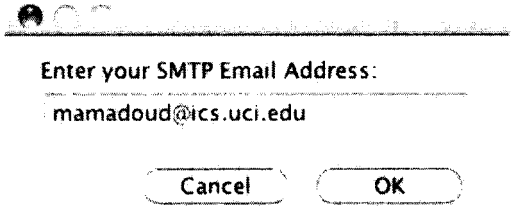

iv.
v. Smtp_auth_user: this is your username for the email you use.



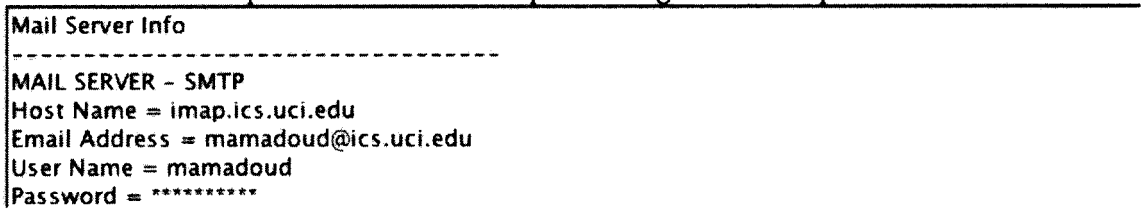

vi. Smtp_auth_pwd: this is the password for the email you use.




vii. SMTP-Email: this is the email address for the email you use.




viii. The information inputted should show up in the right window panel.




c. Backup User Data

This backs up and saves all of your data into the Google Docs account information that you provided information for during the initial setup. The right window should output some text similar to what is shown in the below figure:

```
Uploading Metadata..
 -- clientstate document:1bWPQZuuLDaAP0hzrbQrcNVKOI9e00uu77fn9-IMgt8U
clientstate.txt
 -- DataFunctionOntology document:1Re32gBDh7wzGwv_RybwSBHdHiFNEv8hulm-7CzM_YUg
DataFunctionOntology.txt
 -- DataOntology document:1uWeqOLmbJkvMLwuX7pG6xrwaMhqvuBmBUeKDNGaHBBg
DataOntology.txt
 -- DataTypeOntology document:1s8ZjAPDahWcJrzmWUx9qTJq2pUMrcTSygjnqzUoUJts
DataTypeOntology.txt
 -- FunctionOntology document:1pxVi-obJZsmNGbpb32PzWxD6SXtlDOc5Z71bAkKitHk
FunctionOntology.txt
 -- LearnedAttributes document:1l0ohJfNKGvGm7t_q1Pa0F0m3fkypnnQIsmY7JT-rerM
LearnedAttributes.txt
 -- MappingAttrTechniques document:1ICR1B1Atth7F_1fzrIGDgyLeeFJxUBwbvvgsNlOxj-4
MappingAttrTechniques.txt
 -- MappingTypesTechniques document:1lil24Ndm8vMbaz7KLI5JMK0UJWY8beZ0m7jBH57_wgc
MappingTypesTechniques.txt
 -- operations document:1sn8fhvC9qg0bqEzdwBLmpgXQYdpgTmFWFcjb7387TxE
operations.txt
 -- pairkeys document:1usRBH46BQb6G9LUEKq8hLQZIyeFAb8BjAEQ3I8Ppa-U
pairkeys.txt
 -- policies document:1_qimfmkS18stP2mWjXxAzLG8DgoBaqdjKuxgJCrx-Aw
policies.txt
 -- received document:1Q4DGVxRw1xEWCjt4tFSXq2SI5d9kEP6E1gCJjpJ2i6I
received.txt
 -- serverstate document:1hcTj2Xj4pBIKWz6ykrzgxI2nfMd9yTWT3dxNrV3ybcM
serverstate.txt
 -- shared document:1ULupVx33ZwubdFQfP5gJq0IUQH9PUjWH2smDW8UF8CE
shared.txt
 -- symetrickey document:1CqDcEH903D9DaEw_oDwZYcMyrMgH4dvkndILQ9fB09M
symetrickey.txt
```

d. Restore User Data
This downloads the previously backed up data back into CloudProtect.

e. Display Login Info
This displays both the Google account information inputted into CloudProtect as well as the mail server info that was entered:

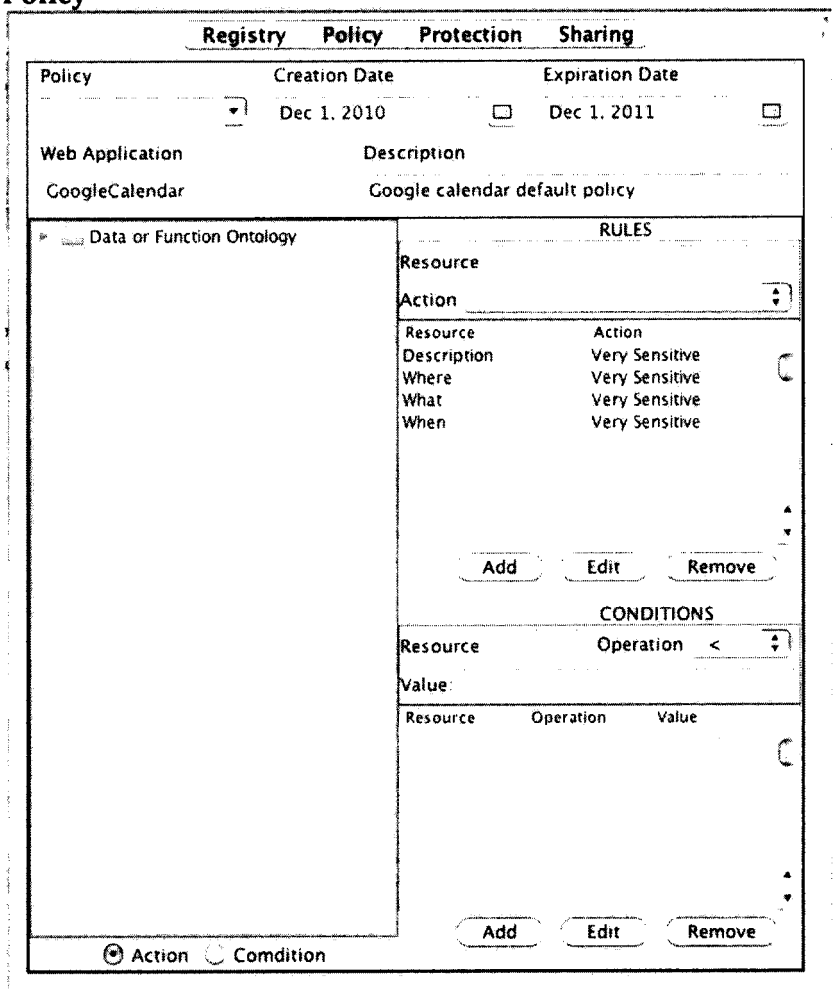
```
GOOGLE
User Name = patricictester@gmail.com
Password = **********
---------------------------------
MAIL SERVER - SMTP
Host Name = imap.ics.uci.edu
Email Address = mamadoud@ics.uci.edu
User Name = mamadoud
Password = **********
```

f. Activate/Deactivate Parser
This is mainly a developer tool. The parser assists in collecting information to implement a new service.

g. Clean All Metadata
This clears all the information stored in CloudProtect.

h. Manage Google Docs
Due to Google security constraints, this part of the application has been built specifically to handle Google Docs encryption.

## III. Policy



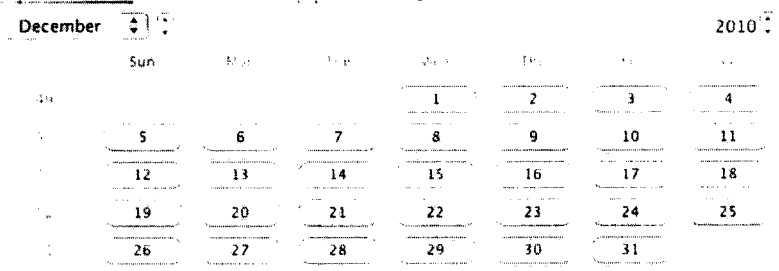

The policy defines what type of encryption will be used. This decides what is encrypted and what is not. Additionally, if certain items can be encrypted, but still need to be able to have actions done on them (e.g. search, translate), these items can be weakly encrypted. All these specifications must be defined here, in the policy. The policy tab must be selected in order to display the window shown above.

a. All fields are mandatory. This means that you cannot leave the policy, creation date, expiration date, web application, or description empty.

b. Policy
Choose a unique name for the policy you want to use.

c. Creation Date

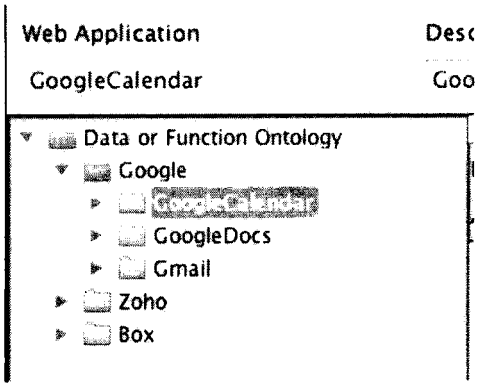
This indicates when the policy was created. Currently this is set to December 1st, 2010. You can choose the date via the date picker as seen below:



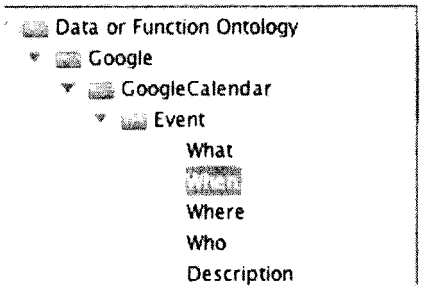

d. Expiration Date
This indicates when the policy will expire. Currently, this is set to December 1st, 2010. You can choose the date via the same date picker you use for the creation date.

e. Description
Choose a short phrase to describe the policy.

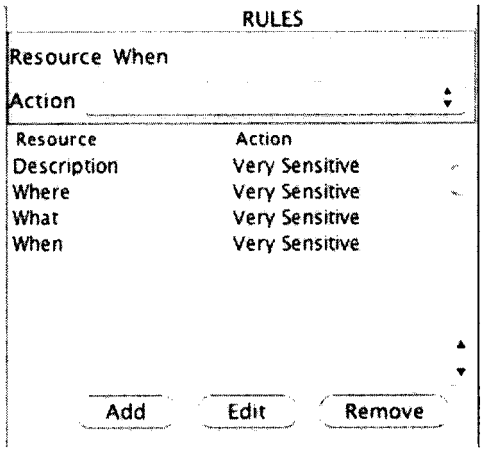
f. Web Application
The web application can be selected from the folder hierarchy shown below the box. Double-click the folder with the name of the service you want to create a policy for in order to select it.




g. Rules
   i. Resource:
   This is the attribute you will be defining a rule for.
   ii. Action:
   First, select an attribute of the object from the file hierarchy. Then choose an appropriate action for that attribute. Depending on what you choose, this will determine whether or not, and how strongly, the attribute will be encrypted. Then, click the Add button to add this mapping to the list of rules.




This figure indicates how to select the attribute. You must expand the folders as seen above to select the attribute. You only need to click on the attribute once to select it.



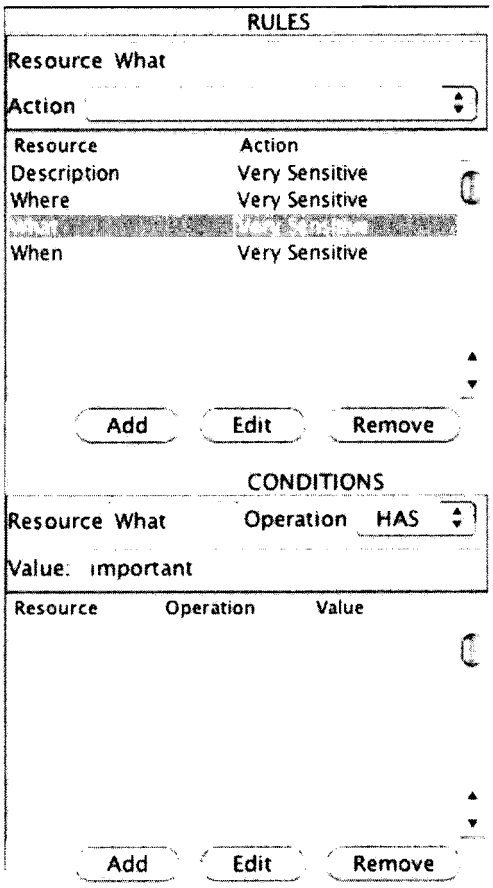

This figure displays the list of rules. You may add, edit, and remove rules from this list.

1. Non-Sensitive
   Non-sensitive items will not be encrypted.

2. Sensitive
   Sensitive items are items that can be encrypted, but still need to be able to have certain actions performed on them (e.g. searching).

3. Very Sensitive
   Very sensitive items can be fully encrypted without causing any errors.

iii. Conditions
The conditions specify when attributes are encrypted. For example, one might only want to encrypt files with the word "important" in them. Make sure that the "Condition" circle is selected. Once it is selected, you can choose which attribute to put a condition on. Note that conditions cannot be added independently, but have to be specified with a rule.




1. Resource
   This indicates which attribute you are performing the condition on.

2. Operation
   Indicates the operation used when being compared to the value. Options are <, <=, =, >, >=, and HAS.

3. Value
   This is the item that is being compared to the attribute.

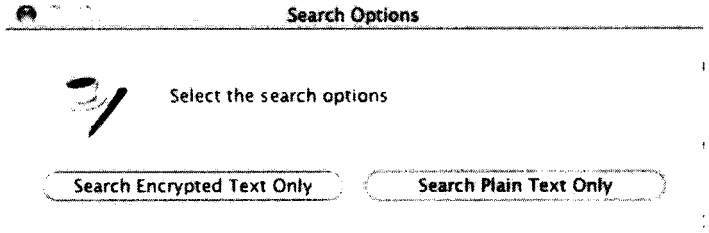
**h. Policy...**

i. Create Private Policy
This creates a blank form with the above components.

ii. Save Privacy Policy
This saves the current policy that you are working on. Be sure to save after you create a new policy or edit an existing one! Your changes will not be saved if you do not select this option from the menu. The text file where this is saved is policies.txt.

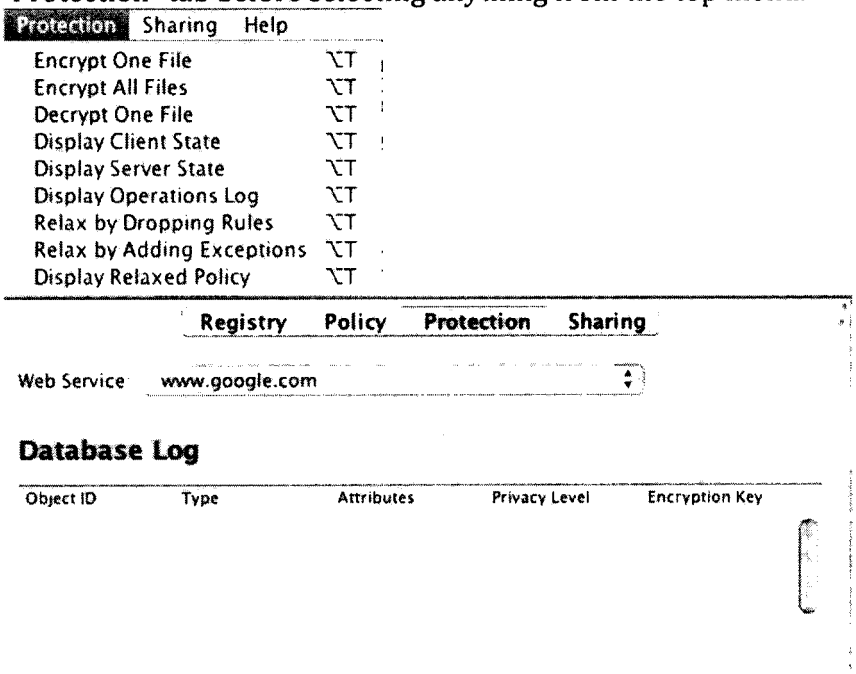
iii. Delete Privacy Policy
This deletes the current privacy policy that you are working on. Be sure you want to delete the policy/are deleting the correct policy, since there are no countermeasures at this point to prevent deletion after accidental clicks.

iv. Search Options
This allows users to search through encrypted text or plain text files.

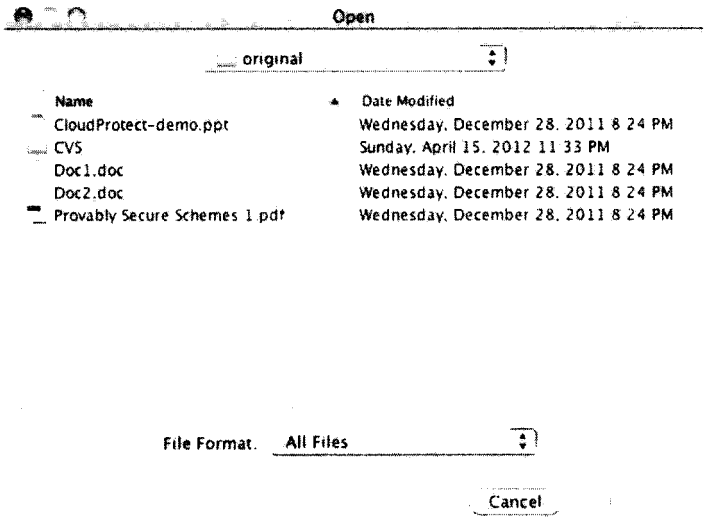



## IV. Protection...

This is where you encrypt local files on your computer. Make sure that you have selected the "Protection" tab before selecting anything from the top menu.




a. Encrypt one file
When you select this, a file chooser will open up and allow you to select one file to encrypt.




Once the file is encrypted, you should see some output similar to this in the right-hand window panel:

```
------------------------------------------------
Original File: Doc1.doc
Web Service: mail.google.com
OBJECT ATTRIBUTES:
Name  Type   Category      Value
------------------------------------------------------------
Author        String  UserData     Mamadou Diallo
Category      String  SystemData   ObjectLevel
CreationDate  Date    UserData     20100723T004200
Name  String  SystemData   Doc1.doc
Title   String  UserData
Type   String  SystemData   DOC
------------------------------------------------------------
PL = 1
Encrypted File: D1E-Doc1.txt
------------------------------------------------
```

All encrypted files are in .txt format. These .txt files can be found under the data/docs/encrypted folder where you downloaded CloudProtect.

b. Encrypt All Files
This allows you to encrypt all the files under a directory that you select.

c. Decrypt One File
This decrypts your original file. You can find this file under data/docs/decrypted. If decryption does not succeed, the original file is also stored under data/docs/original.

d. Display Client State

This displays various bits of information regarding actions you have done locally on your own computer (without the usage of any external services). After setting up a policy and encrypting a file, the information displayed should look something like this:

CLIENT PROCESSED OBJECTS
---
Object ID = D1E-Doc1.txt
URL = mail.google.com
Data Type = doc
Encryption Key = Ï›◊„eÜ‹≥9?È4ë
Cost = 1086
Author [0], Content [1], CreationDate [0], Title [0],
Privacy Level = 1
Policy Rules:
  Content: [1001510212]
---
Object ID = D1E-CloudProtect-demo.txt
URL = mail.google.com
Data Type = ppt
Encryption Key = É±ÌY›\Úî•?<t
Cost = 763
Author [0], Content [1], CreationDate [0], Title [0],
Privacy Level = 1
Policy Rules:
  Content: [1001510212]
---

e. Display Server State
This displays information regarding actions done by the outside services used in junction with CloudProtect. The parser needs to be turned on, or activated, in order to receive any information to display here. If there was nothing done with the outside services, the right-hand window should only display something like this:

Web Service: mail.google.com

f. Display Operations Log
This shows information regarding operations you have done on an external service. Again, the parser needs to be turned on, or activated, to receive information to display. If you have not done any operations, the right-hand window should only display something like this:

Web Service: mail.google.com