tech doc

iQ Suite

Using CORE for SPAM Recognition in securiQ.Wall Version 7c or higher

Valid as of iQ.Suite 7c for Domino. For previous versions (up to 7b), please read "CORE_configuration_in_Wall_en.pdf".

GROUP TECHNOLOGIES

Contents

1 Text Analysis Using CORE - Introduction

In text analysis based on **CORE Technology**, contents are not checked against wordlists, but "learned" as vector through a text representation, so that messages and documents with texts of the same category can later be identified without using wordlists at all. CORE is independent of word-lists or dictionaries and works with all European languages. Because the senders of SPAM tend to work with continually changing (even non-existing) e-mail addresses and content, this technology is especially useful for **blocking SPAM**.

As for a dictionary-based analysis, the **Text Analyzers** and **Converters** are used to categorize the texts and convert them into ASCII format.

To analyze messages and documents with CORE, a representative reference set of mails (SPAM, newsletters, business correspondence, etc.) is copied into a database. For this purpose, GROUP provides a database – **g_learn.nsf**, located in the **grptools** directory – in which documents can be stored and categorized. In training mode, a securiQ.Wall database job "learns" your categories and creates a classifier. In analysis mode, a securiQ.Wall database job then categorizes them for checking. If the checking procedure was successful, activate a securiQ.Wall mail or database job that applies this classifier to all documents, so that all messages and documents with content defined as undesirable are filtered.

2 Setting Up Text Analysis Using CORE

2.1 Procedure

1. Create a reference set of company-typical e-mails
2. Categorize these mails in a training database
3. Configure Analyzers
4. Create a "Teaching-Job"
5. Check the result with a "validation job"
6. Adjust categorization where required
7. If successful, set up final CORE job

2.1.1 Creating the Reference Set of E-Mails

The easiest way to create a reference set of e-mails is to set up a securiQ.Wall job that copies all incoming e-mails to a separate quarantine database without blocking them.

Please note that this job needs to be run prior to your standard securiQ.Wall job and therefore requires a higher priority.

Proceed as follows:

- Create a copy of the quarantine database: **g_arch_sammler.nsf**
- Activate a securiQ.Wall job to collect mails with the following settings:
  - For mails from Internet
  - Without deleting the documents
  - Without notification
  - To be stored in the previously created copy of the quarantine database: **g_arch_sammler.nsf**

To collect the mails, use the pre-configured job **CORE: Collect Mails from Internet** and adjust it to your requirements.

2.1.2 Collecting and Categorizing the Mails

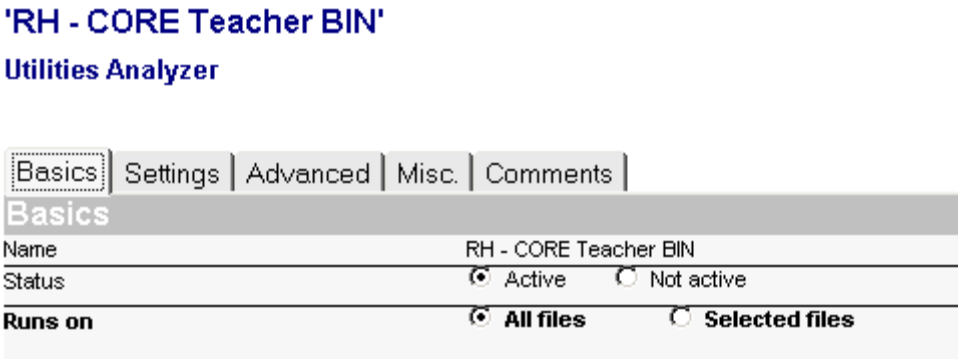
- Collect mails in the **g_arch_sammler.nsf** quarantine database for at least one night.
- Select a typical set of mails from this database and copy them to the **g_learn.nsf** training database. Only select mails without attachments at this point.
- Categorize the mails manually. For details on how to categorize the mails, please refer to training database online help (Click on **Help** in the **g_learn.nsf** database).
  - Regarding the training database, observe the following:
    - **Copy** the documents to the training database; if they are forwarded, the mail contents will be falsified!
  - Regarding the categories, observe the following:
    - Categorize the mails into two categories, e.g. SPAM, NOSPAM
    - Category names must be entered in upper case letters, without blank, colon or backslash.
    - Select at least 10 documents for each category. A minimum of 100 documents per category is recommended. Assigning more than 500-600 documents to a category will not significantly improve the recognition rate

2.1.3 Configuring the Analyzers

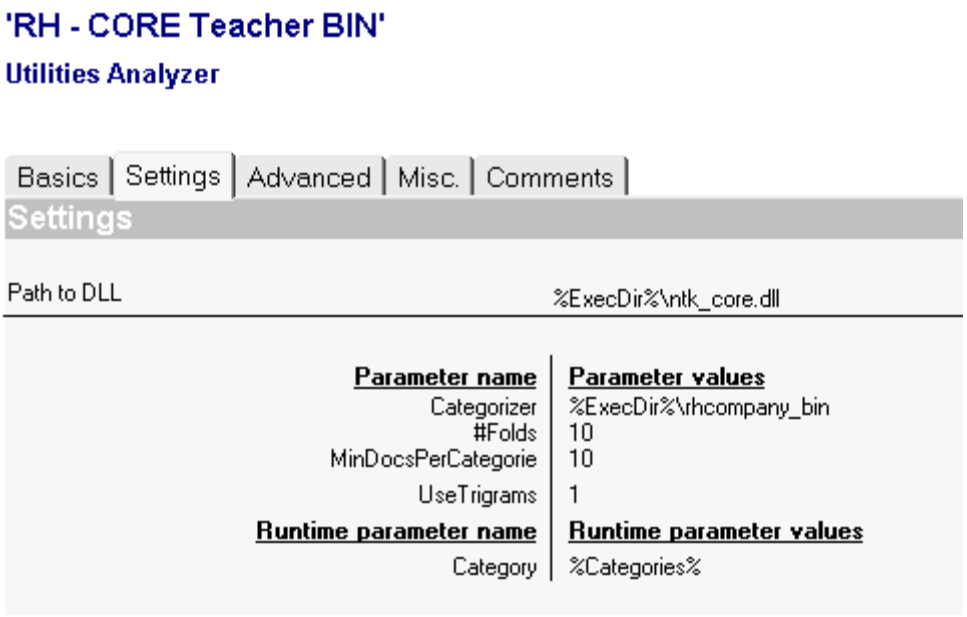
Follow the instructions below to create the text analyzers (training and analysis) for the company-specific classifier:

- Select: **securiQ → Wall → Utilities → Text Analyzer**:

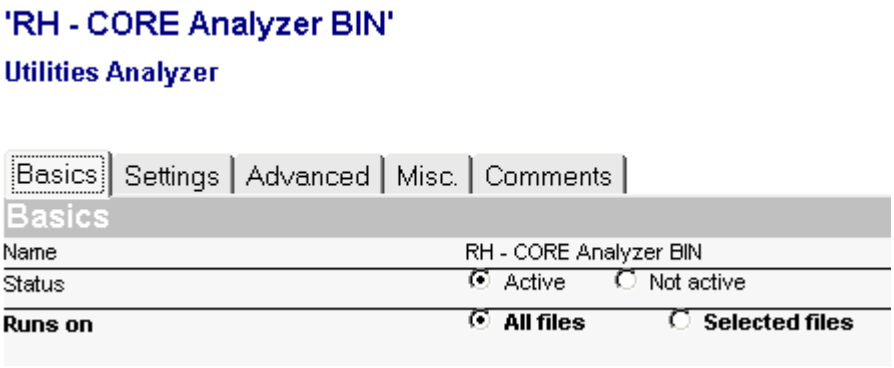
- Copy the existing **CORE Teacher** (be sure to select the correct operating system!) and adjust it.
  - Assign a new name:
    e.g. <company name or acronym> – CORE Teacher



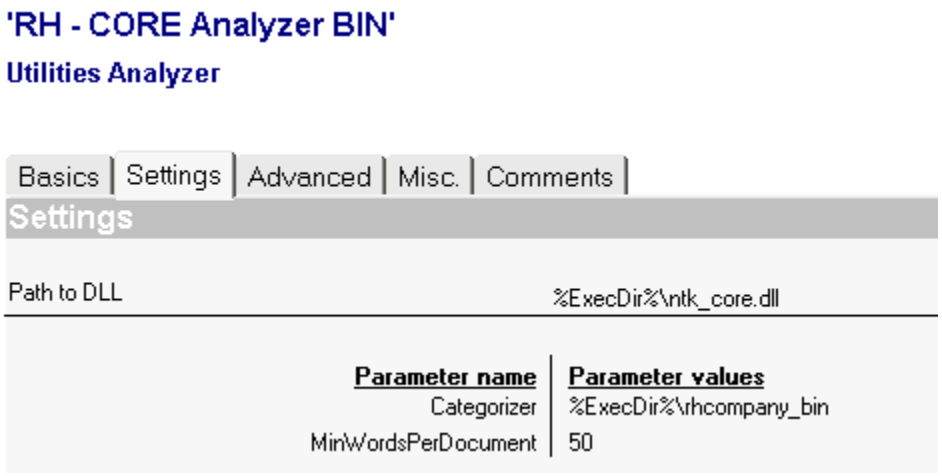
- Under **Settings**, assign a name to the **Categorizer**:
  e.g. <company name or acronym >



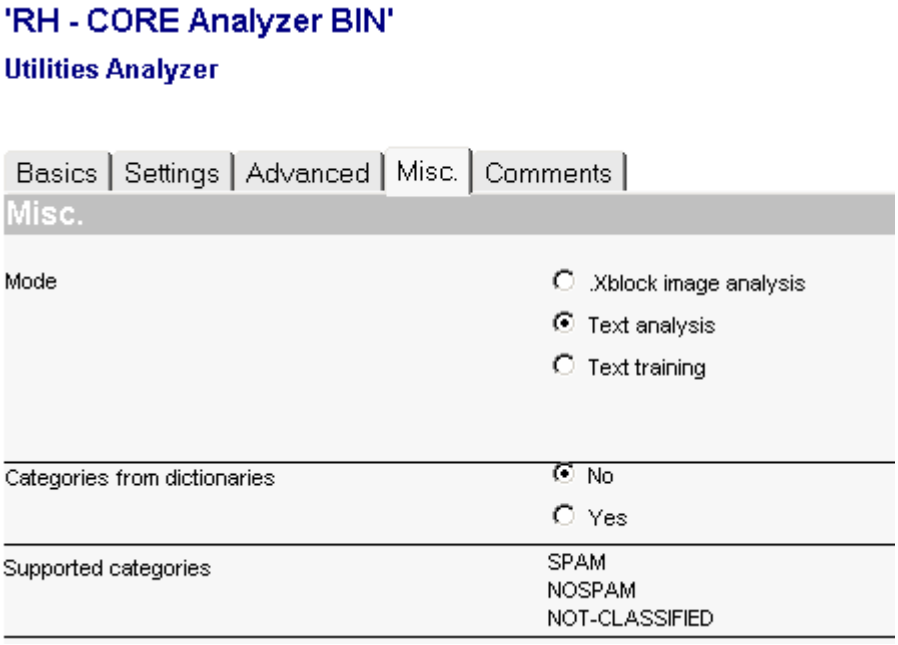
- Copy the existing **CORE Analyzer** and adjust it:
  - Assign a new name:
    e.g. <company name or acronym> – CORE Analyzer



- Under **Settings**, assign a name to the **Categorizer**:
  e.g. <company name or acronym>. The name has to correspond to the name assigned to the **CORE Teacher**.



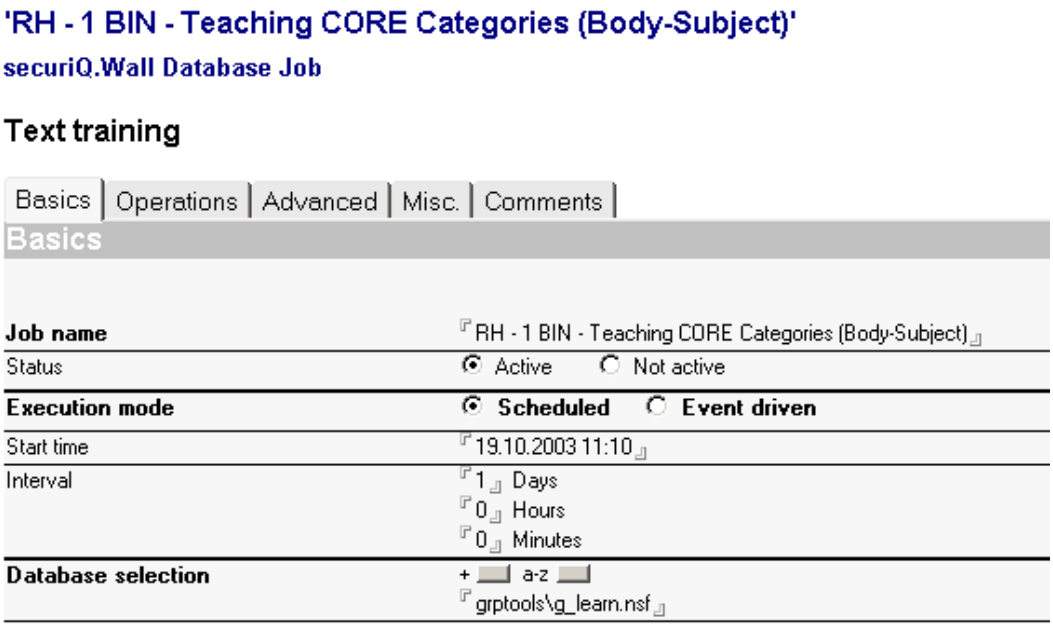
- Under **Misc**., enter all categories defined in the training database in the **Supported Categories** field:
  e.g.:



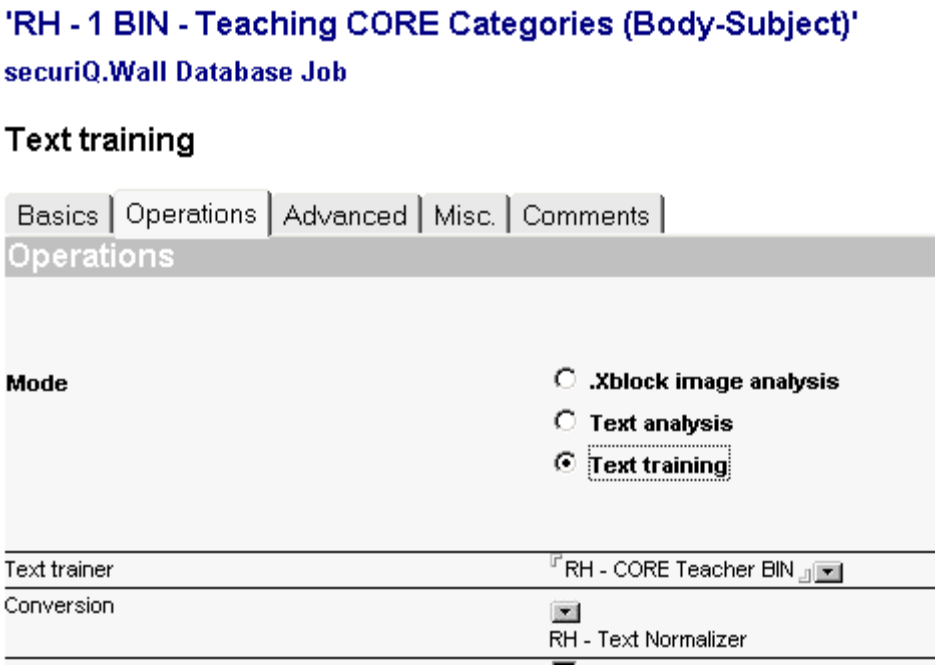
Define a unique category to take care of the documents not covered by the Classifier, e.g. a NOT-CLASSIFIED category. If new categories are added in a subsequent training run, be sure to update the Analyzer accordingly! Only the categories entered in this field can be selected from a list when the job is created.

2.1.4 The "Teaching Job" – Creating a Classifier

- Copy the securiQ.Wall database job **1- Teaching CORE Categories (Body-Subject)** and adjust it:
  - Assign a new name
    e.g. <company name or acronym> – Teaching CORE Categories (Body-Subject)

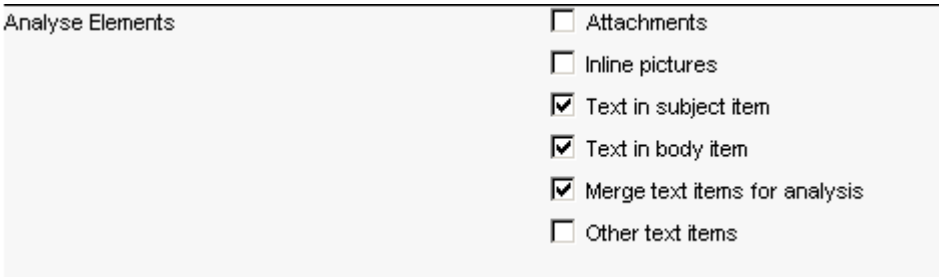


- Under **Operations**, enter the previously defined text analyzer for the teaching process in the **Text training** field:
  <company name or acronym> CORE Teacher



Within the teaching job, the CORE Teacher is applied to all categories defined in the training database. It is not possible (and not useful) to "learn" only some the categories of the training database.

- In the **Analyze Elements** field, select the e-mail fields to be analyzed.



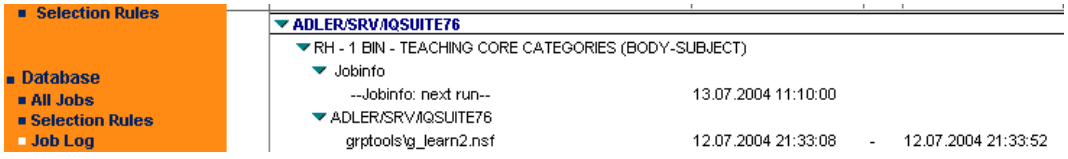
To identify SPAM, it is not necessary to analyze attachments, as this kind of mail is currently not sent with attachments. Excluding attachments avoids unnecessarily increasing the server load.

If you want to use CORE for more than blocking SPAM and therefore wish to analyze attachments as well, you need a (further) classifier that was specifically trained to analyze mails with attachments, as their structure is different from those without attachments. In that case, you need to create two training databases, one for mails with attachments and the other for mails without attachments. You also need two text analyzers for the training process and two for the analysis process, two securiQ.Wall database jobs for teaching and two securiQ.Wall mail Jobs for analysis – one for mails with attachments and one for mails without attachments. One job only processes mails without attachments and analyzes the subject line and the body text, while the other only processes mails with attachments and processes the attachments in addition to the subject line and the body text.

In the job, specify the analyzer designed to process mails with attachments. In addition, specify three converters (in the order below) in the **Conversion** field:

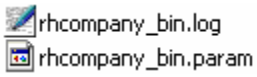
1. File to XML Extractor
2. XML to Text Converter
3. Text Normalizer

- Check if the teaching job was completed correctly:
  - Two documents are created in the **Job Log** for a completed database job:



    - --Jobinfo: next run--
    - run from ... to...

- In the **grptools** directory on the server, you will find two new files of the same date:
  - < company name or acronym>.param: the classifier for the analysis using CORE
  - < company name or acronym>.log: the log file of the teaching process



- If run successfully, deactivate the teaching job.

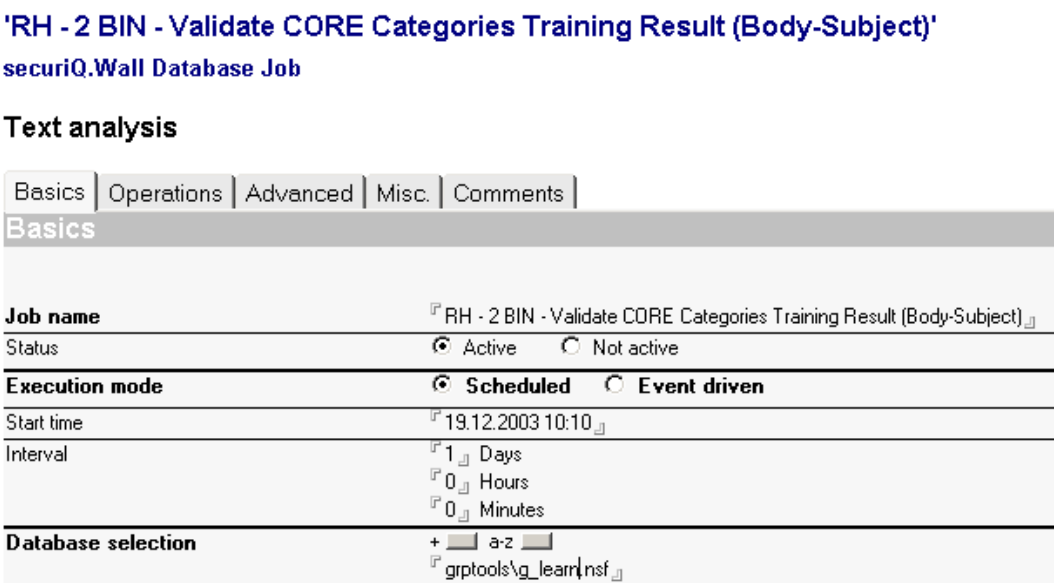
2.1.5 The "Validation Job" – Checking/Testing the Classifier

The initial check of the classifier created by the training job should be performed using a "validation job" or securiQ.Wall database checking job. A further possibility is to have a securiQ.Wall mail job use the classifier to analyze the incoming mail and check the results obtained.

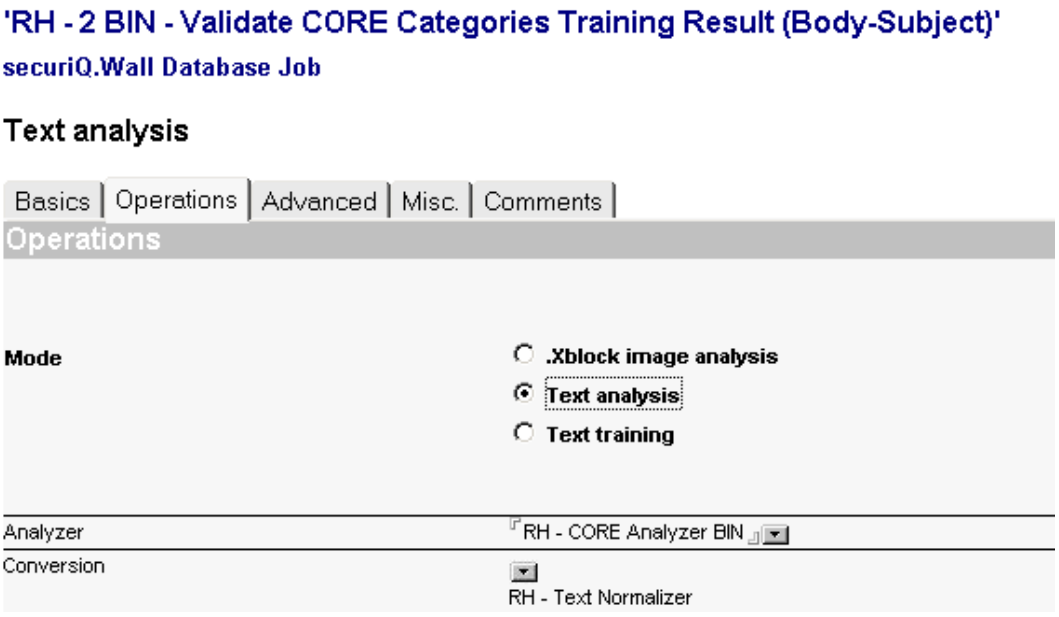
- Checking the classifier with Wall database "validation" or checking job:
  - Before running the validation job on the training database, set the following ToolKit parameter in the **Notes.ini** file:
    `ToolKit_DBGrabberOpenExpanded=YES`
    The parameter can be set using the “set config” console command or in the iQ.Suite Global Parameters.

  - Copy the securiQ.Wall database job **2 - Validate CORE Categories Training Result (Body-Subject)**, then adjust and enable it:

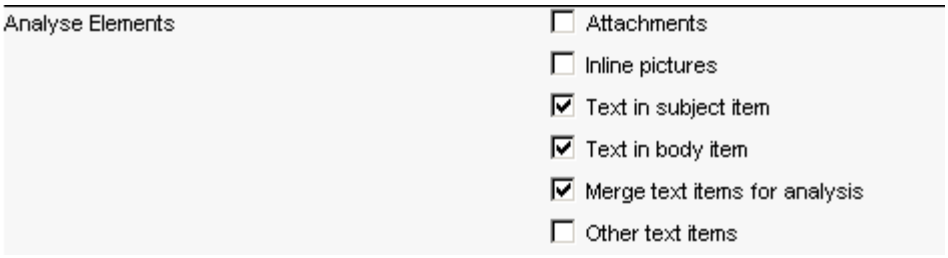
    - Assign a new name
      e.g. *<company name or acronym> – Validate CORE Categories Training Result (Body-Subject)*



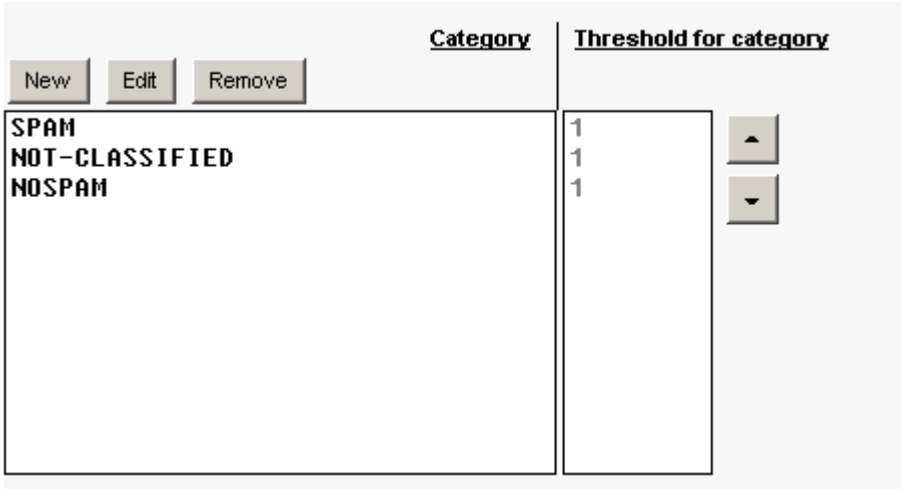
☐ Under **Operations**, enter the **Text Analyzer** previously defined:
<company name or acronym> CORE Analyzer



☐ In the **Analyze Elements** field, select the same settings as for the teaching job:



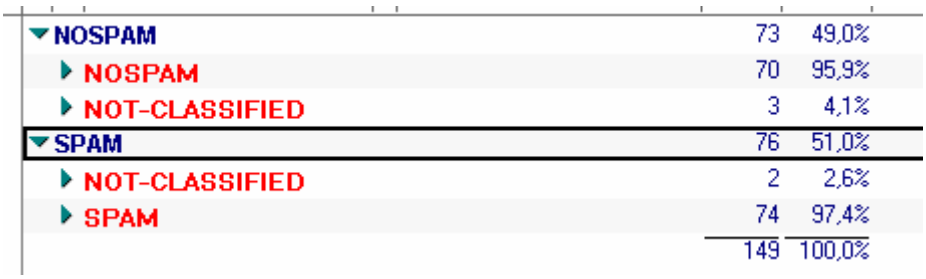
☐ In the **Categories** field, enter all analyzer categories with the threshold set to 1:



Click on **New** to add further categories. To change an existing category, select it and click on **Edit**.

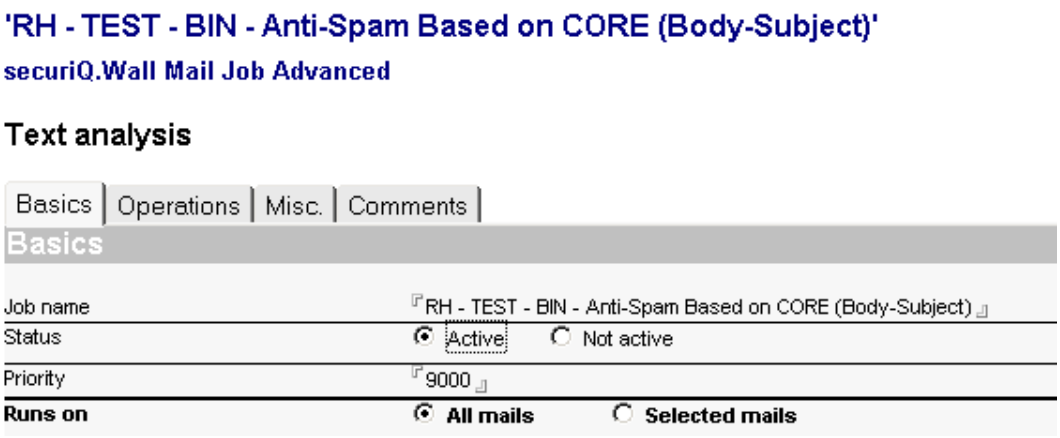
☐ Run the job. The job will now check all mails in the training database and automatically reassign them to the categories.

- The results determined by the job are shown in the training database as further categories (in red):



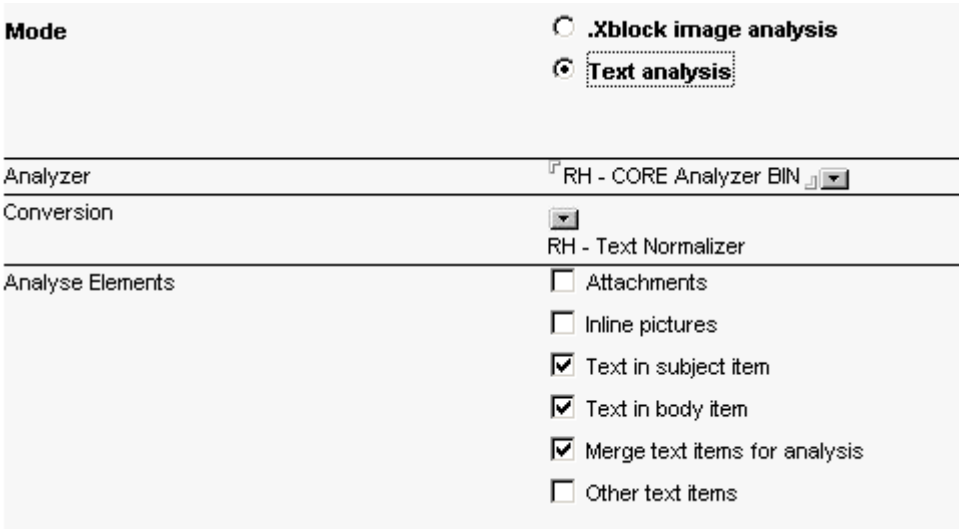
In this example above, the validation job has correctly identified (100%) all categorized mails. The documents categorized under NOT-CLASSIFIED have not been taken into account when creating the classifier. Now test the classifier with a Wall mail job that checks the mail traffic.

- Testing the classifier with a securiQ.Wall Advanced Mail Job:
  - Set up a Wall Advanced Job.
    - Assign a name, e.g.
      <company name or acronym> - TEST Analysis with CORE

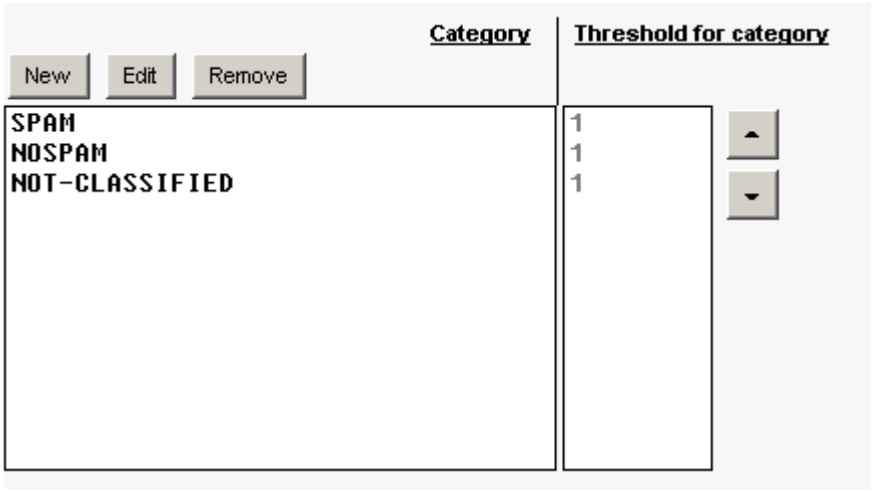


Assign a higher priority than for your standard content checking job and run the job on all mails.

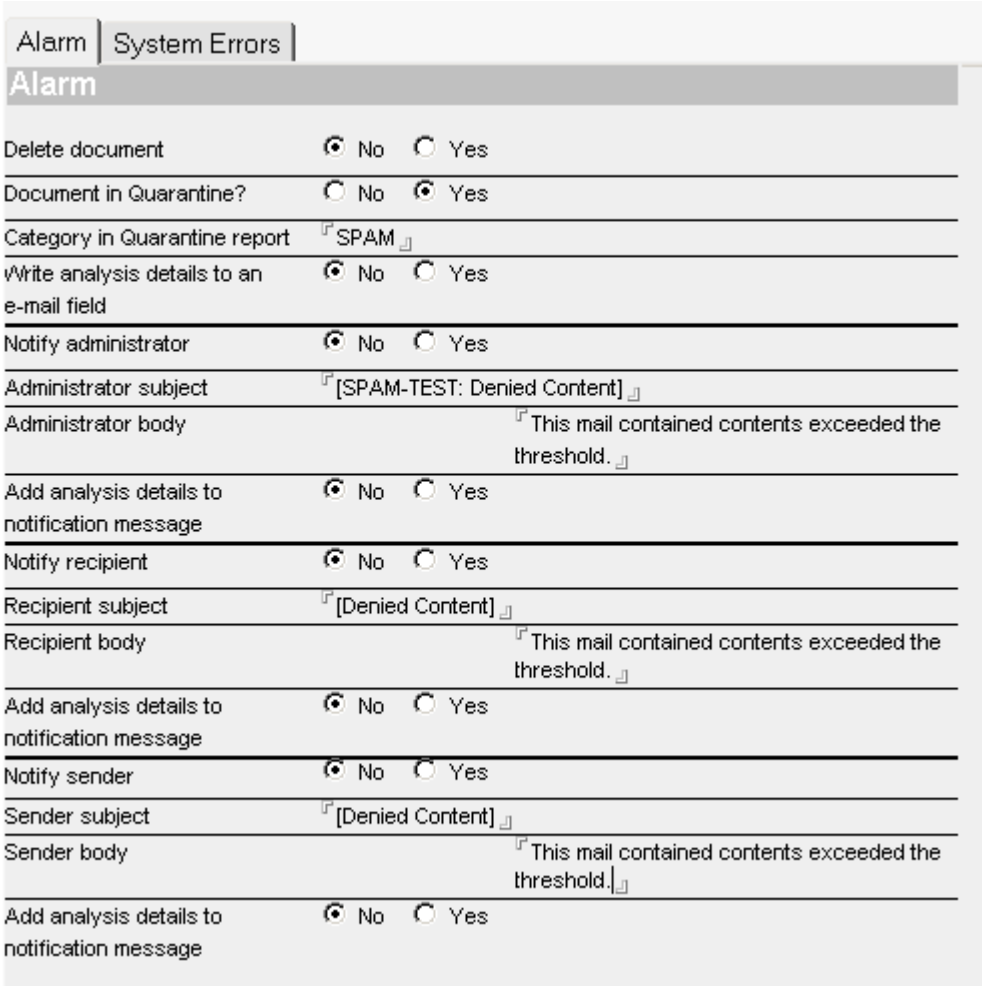
☐ Under **Operations**, enter the CORE Analyzer created:
<company name or acronym> CORE Analyzer



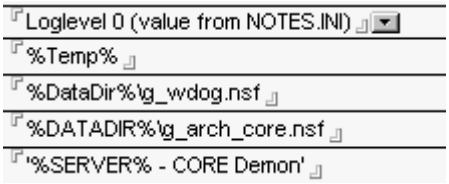
☐ Enter **all** categories with the threshold set to 1, in order to check whether or not each mail is assigned to the correct category:



☐ Let all documents be normally delivered and not deleted. Also disable all notifications, except for those to the Administrator in case of an error (in the **System Errors** tab).



- ☐ Create a copy of the quarantine database and name it **g_arch_core.nsf**. In the **Misc**. tab, select the separate quarantine database (**g_arch_core.nsf**). All mails will be copied to that database:



- ☐ Activate the job.

- ☐ After some time, check the result in the quarantine database (View **Originals – With Body**): If the result is unsatisfactory (e.g. business mails classified as SPAM), adjust the categorization (see section below).

2.1.6 Adjusting the Categorization

Repeat the following steps as often as required, i.e. until the classification performed by the test job is satisfactory. The goal should be that no business mail is classified as SPAM.

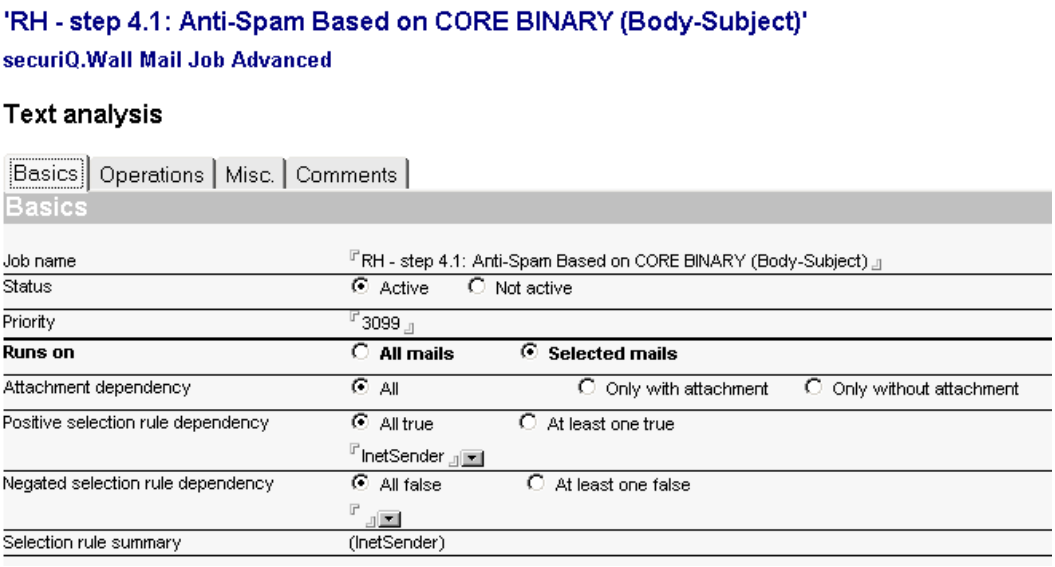
1. Copy the mails wrongly categorized to the training database and assign the correct category.
2. Disable the Wall mail test job.
3. Delete the job log of the database jobs.
4. In the quarantine database, delete all documents for the test job
5. Activate the Wall database teaching job.
6. Check the job log to make sure the teaching job has been completed correctly.
7. After having run the teaching job, disable it and re-run the Wall mail test job.
8. After some time, check the result in the quarantine database (View **Originals – With Body**): If the result is unsatisfactory (e.g. business mails classified as SPAM), go back to Step 1.

9. After several runs, you should check whether the documents in each category are still fairly "similar", e.g.:
   - NOSPAM: business mails or newsletters
   - SPAM: MIME mails

- To obtain a better view of the test job results, use the Designer to adjust the quarantine database as follows:
  In the Originals views, insert an additional column (after the categories) to display the analysis result: (@Word(Check_Details;"=";1)).

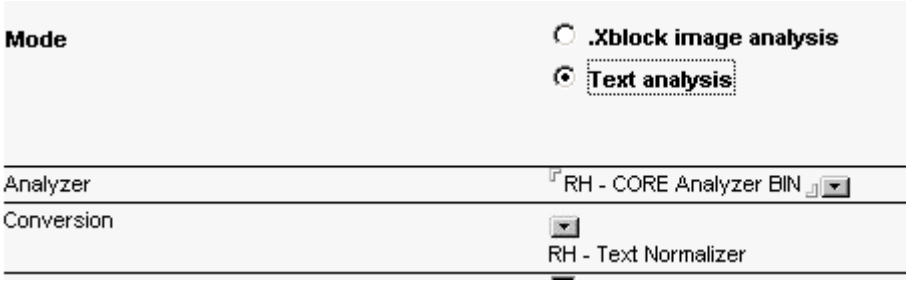
2.1.7 Activating CORE Analysis for Incoming Mails

- Copy the securiQ.Wall mail job **Anti-Spam Based on CORE (Body-Subject)**, then adjust it and finally enable it:
  - Assign a new name
    e.g. *<company name or -acronym> – Anti-Spam Based on CORE (Body-Subject)*

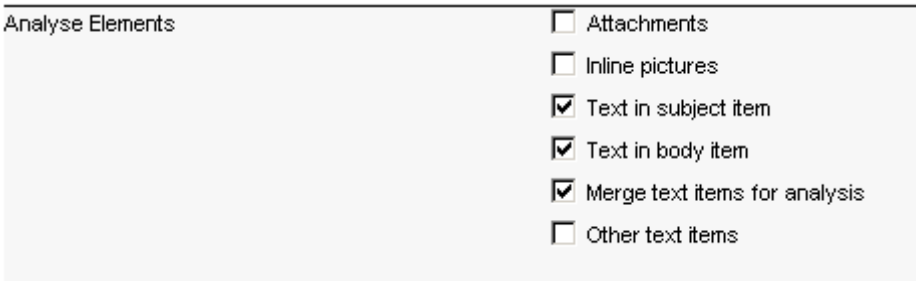


The job is run on all incoming Internet mails with the **InetSender** selection rule.

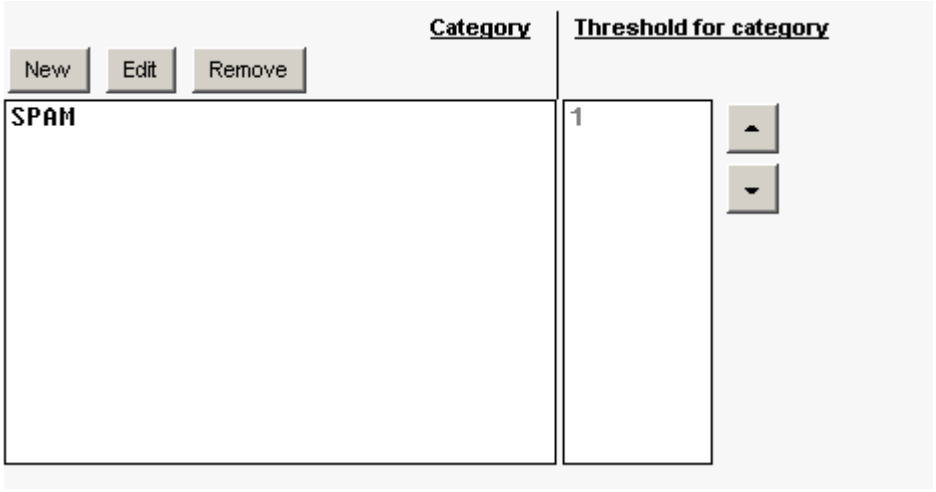
- Under **Operations**, enter the **Text Analyzer** previously defined:
  <company name or -acronym> CORE Analyzer



- In the **Analyze Elements** field, select the same settings as for the teaching, validation and mail checking jobs:



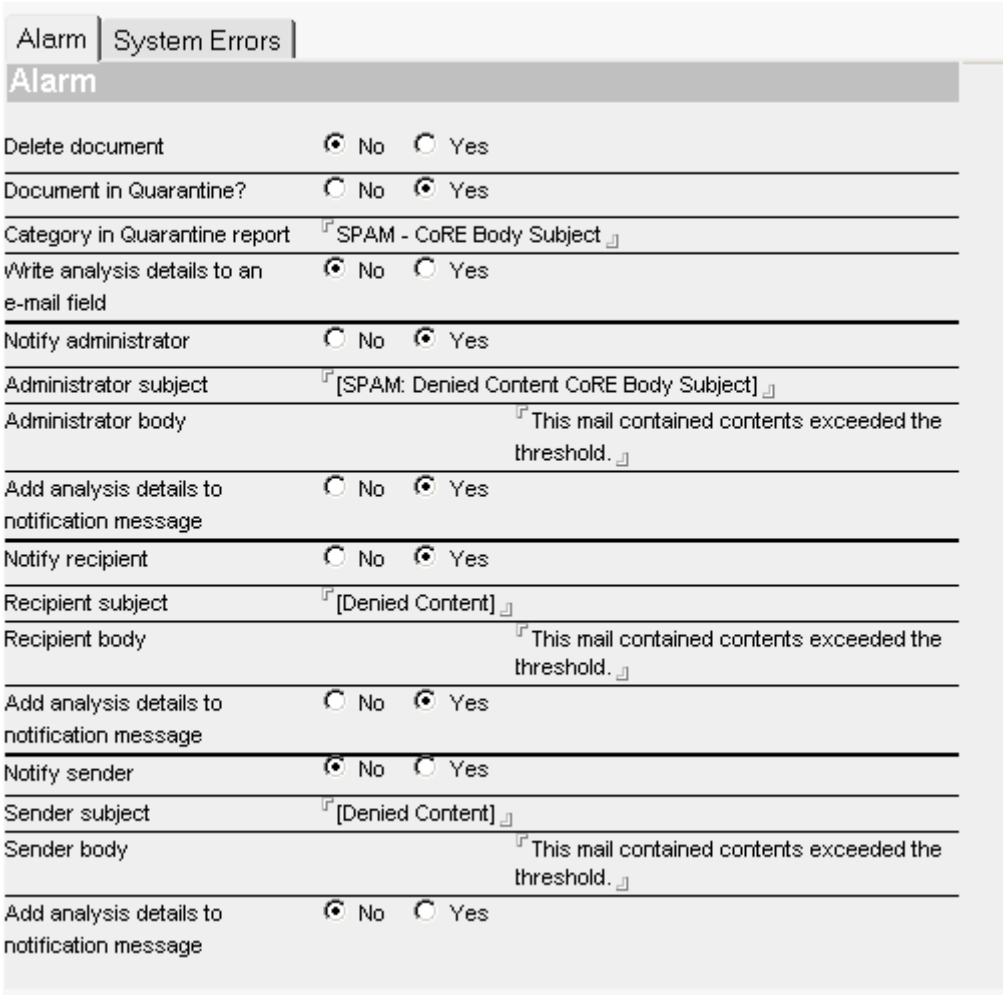
- In the **Categories** field, enter the **categories to be blocked** with the threshold set to 1:



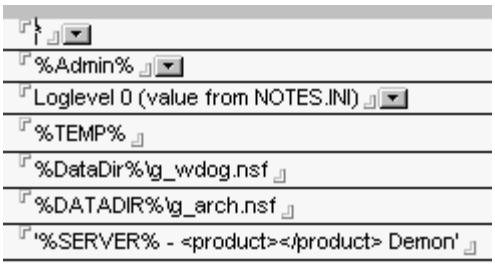
Click on **New** to add further categories. To change an existing category, select it and click on **Edit**. To delete a category, select it and click on **Remove**.

Only enter the mail categories the recipients are not supposed to receive, i.e. typically SPAM! Remove any other category from this screen.

☐ Let the documents be deleted and moved to the quarantine. Define a meaningful category for the quarantine. Enabled notifications on both the **Alarm** and **System Errors** tabs as required.



☐ In the **Misc**. tab, enable your usual quarantine database (typically **g_arch.nsf**):



- After some time, check the result in the quarantine database (View **Originals – With Body**): If the result is unsatisfactory (e.g. business mails classified as SPAM), readjust the categorization.

2.2 Procedure in a Replicated Environment

In a replicated environment with two or more servers, you have two different options:

1. Run the teaching process on one server and then copy the classifier file **<company name or acronym>.param** to the `grptools` directory of the other servers. This classifier will then be used by the analysis jobs.
2. Run the teaching process on each server, i.e. replicate the training database with the categorized documents on the other servers. The teaching job will then be executed on each server with the same reference set.

Then proceed as described in Sections 2.1.1 through 2.1.5.

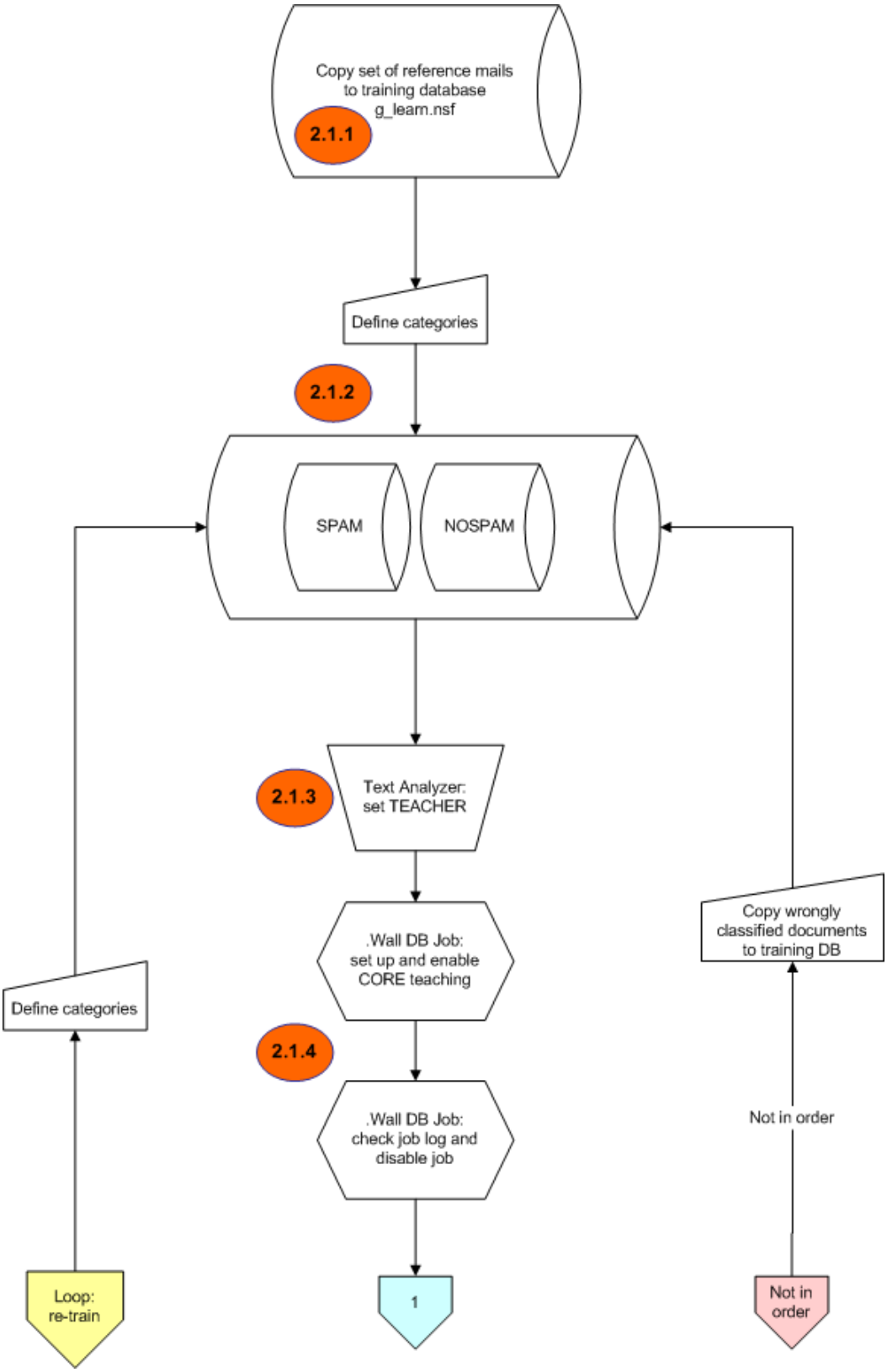
Further settings in a replicated environment include the following:

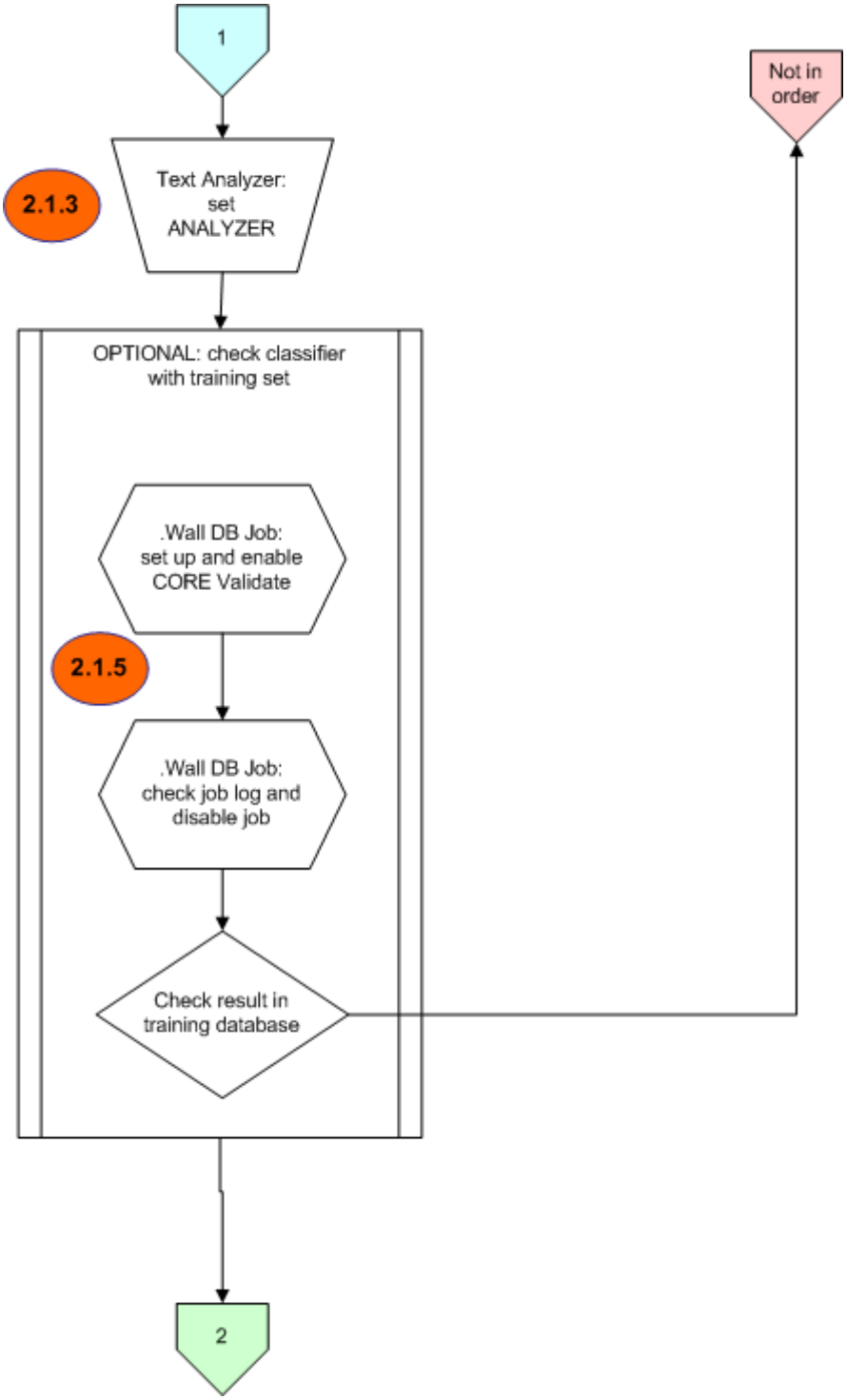
2.2.1 Additional Settings in a Replicated Environment

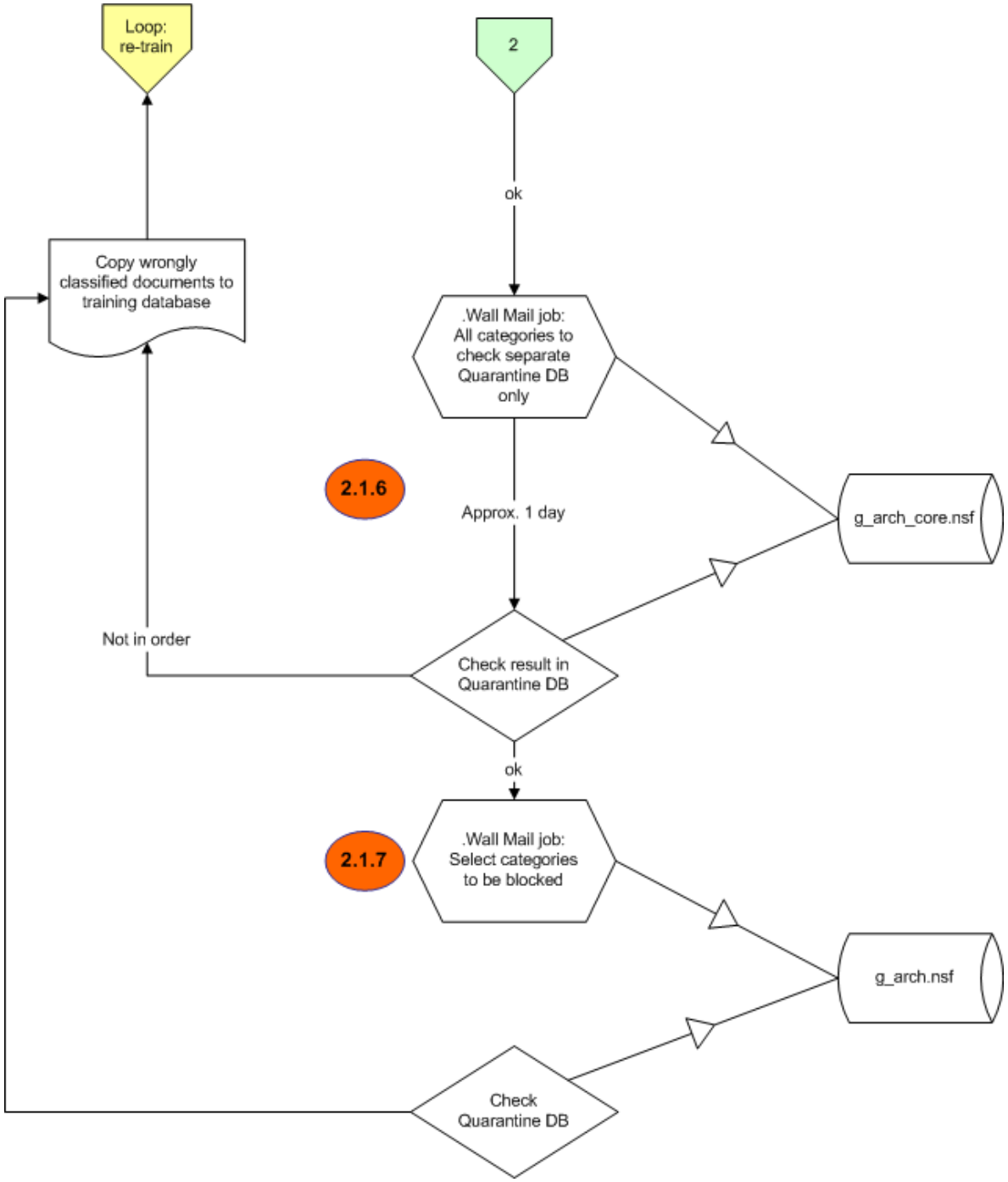
Repeat the following steps as often as required, i.e. until the classification result is satisfactory:

1. Copy wrongly categorized mails to the training database and assign the correct category.
2. Disable the mail test job
   → Replicate the `grptools` directory with the second server.
3. Delete the job log of the database jobs.
4. In the quarantine database (**g_arch_core.nsf**), delete all documents for the test job.
5. Run the database teaching job
   → Replicate the `grptools` directory with the second server.
6. Check the job log to make sure the teaching job has been completed correctly (on both servers!).
7. After having run the teaching jobs on both servers, disable them and re-run the Wall mail test job.
   → Replicate the `grptools` directory with the second server.
8. After some time, check the result in the quarantine database (View **Originals – With Body**): If the result is unsatisfactory (e.g. business mails classified as SPAM), go back to Step 1.

2.3 Flow Chart


Copy set of reference mails to training database g_learn.nsf
2.1.1
Define categories
2.1.2
SPAM
NOSPAM
2.1.3
Text Analyzer: set TEACHER
.Wall DB Job: set up and enable CORE teaching
2.1.4
.Wall DB Job: check job log and disable job
1
Define categories
Loop: re-train
Copy wrongly classified documents to training DB
Not in order
Not in order


1
Not in order
2.1.3
Text Analyzer: set ANALYZER
OPTIONAL: check classifier with training set
.Wall DB Job: set up and enable CORE Validate
2.1.5
.Wall DB Job: check job log and disable job
Check result in training database
2


Loop:
re-train
2
ok
Copy wrongly classified documents to training database
.Wall Mail job: All categories to check separate Quarantine DB only
2.1.6
Approx. 1 day
g_arch_core.nsf
Not in order
Check result in Quarantine DB
ok
2.1.7
.Wall Mail job: Select categories to be blocked
g_arch.nsf
Check Quarantine DB

3 About GROUP Technologies AG

GROUP Technologies AG is one of the world's leading manufacturers of e-mail security, organization and management software. The company's innovative products have made GROUP one of the technological leaders in these areas. Optimally coordinated, the iQ.Suite products are available for Lotus Notes, Microsoft Exchange and SMTP platforms.

GROUP's portfolio ranges from e-mail cryptography and virus protection to anti-spam and secure archiving of e-mails, all out of one hand and in superior quality. Using GROUP's iQ.Suite enables companies to reduce cost, optimize the efficiency of their e-mail environment and raise work productivity.

iQ.Suite is modular, scalable company-wide and offers customers the required degree of investment security. Through its fully server-based architecture, iQ.Suite can be administered centrally and economically.

GROUP Technologies AG's customer base includes a wide variety of renowned companies, such as Deutsche Bank, Ernst & Young and Honda. iQ.Suite is available from GROUP directly and via OEM or trade partners. Over five million users utilize GROUP Technologies AG products to protect their systems.

GROUP Technologies AG is headquartered in Karlsruhe, Germany. The company maintains offices internationally both in Europe and in Boston, Mass., USA.

www.group-technologies.com

The product descriptions are general and descriptive in nature. They can be interpreted neither as a promise of specific properties nor as a declaration of guarantee or warrantee. The specifications and design of our products can be changed at any times without prior notice, especially to keep pace with technical developments.

The information contained in this documentation deals with issues as assessed by GROUP Technologies AG at the time of publication. As GROUP Technologies AG is bound to react to changing market requirements, this document by no means represents an obligation by GROUP Technologies AG and GROUP cannot guarantee the correctness of the information presented in this document after its publication.

This documentation is intended for information purposes only. GROUP Technologies AG hereby excludes any warranty, express or implied, for this document. GROUP Technologies AG is unable to guarantee, either explicitly or tacitly, the quality, execution, standardization or suitability for a specific purpose.

All product or company names in this document may be protected brand names of their respective owners.

Headquarters
GROUP Technologies AG
Ottostrasse 4
76227 Karlsruhe / Germany
Phone +49(0)721-4901-0
Fax +49(0)721-4901-199
info.de@group-technologies.com
www.group-technologies.com

North American Headquarters
GROUP Technologies
321 Fortune Blvd.
Milford, MA 01757/USA
Phone +1 508-473-3332
Phone 877-476-8755 (US and Canada)
Fax +1 508-473-9940
info.us@group-technologies.com
www.group-technologies.com