Configuring GEM – A Primer

Easier than you think

GEM gives you multiple options for configuring 'group' rules. That is, a single rule that covers multiple people or multiple organizations or multiple business classifications. This is a very important concept.

- You do not need to have a rule for each employee.
- You do not need to have a rule for every customer.
- You do not need to have a rule for every business classification.

Theoretically, you could get by with a single rule covering all employees but in reality that won't work because of the need to assign appropriate security classifications to emails. In the following example we will show you how you can analyze, capture and classify all emails to and from your employees (internal and external emails) with just 16 rules. These same 16 rules would work equally well for an organization with 100 employees as for an organization with 10,000 employees.

Why do we want to minimize the number of rules we use?

In any business, private or government, things change over time. Organizations grow and contract and split and merge and employees come and go. This means that rules need to be maintained. The less the number of GEM rules you have the lower your maintenance workload. We manage all of our emails with just 16 rules and we could probably do it with less. If you create a large number of rules you are also creating a much bigger maintenance task.

GEM includes clever functionality to allow you to capture most emails with group rules. These group rules can be:

1. Employee-centric;
2. Customer-centric;
3. Classification-centric; or
4. Any combination of the above.

The example in this paper is employee-centric.

It doesn't matter which rule type you choose (i.e., employee, customer or classification) because any one can capture all of your emails. And, once the emails are in the RecFind 6 database, they can be securely accessed, enterprise-wide using our sophisticated search functions. In RecFind 6 you can search for emails on any component of the email (e.g., sender, recipient, subject, text of the email, text of the attachment, etc) regardless of what type of rule you have used to capture emails.

Basically, as long as you have the required security you can easily and quickly search for and find any email stored in RecFind 6 regardless of how it was initially classified.

This is really what you need to do; you need to capture all valid corporate emails, store them in an inviolate state in the database (so they can't be changed by end-users) and then provide access via your corporate security regime making sure people only get to see emails they are authorized to see.
The database then becomes both an invaluable information resource (an instantly accessible source of knowledge) and an email archive for the purpose of all compliance legislation.

There is a sequence of steps you need to go through to properly configure employee-centric rules in GEM.

1. You can't begin to define rules until you know and agree on exactly what it is you want to achieve. So, please talk, discuss and agree BEFORE you start configuring GEM.
2. Agree on security. When we store emails in GEM we give every email a security code that determines who can see it and who can't see it when searching in RecFind 6. For example, agree on a security classification system like the following - Directors, Managers, Sales, Support, Administration, Marketing, R&D, etc. Then agree on who can see what - for example, directors can see everything but support people can only see support emails. Sales people can see sales and support and marketing emails, etc. Get this aspect clear and agreed before configuring rules otherwise you will end up doing a lot of rework. Once agreed, configure your security classifications in the RecFind 6 DRM. If you are already a RecFind 6 user then simply use the security rules you already operate under. One set of security rules should apply to all 'documents" no matter what the form (e.g., emails, electronic documents and paper).
3. Agree on what constitutes a valid corporate email and what constitutes a 'private' email. Most organizations allow some degree of private usage of the email system. There are also a plethora of laws and regulations (differing by organization, state and country) that specify how 'private' email must be handled. Because there is no real way a computer program can read the text of an email and decide if it is private or not (e.g., an invitation to lunch could be private or business) the easiest way to handle this thorny issue is to tell all employees that private emails will only be recognized if they have specified text in the subject line, e.g., "Privateemail". Then

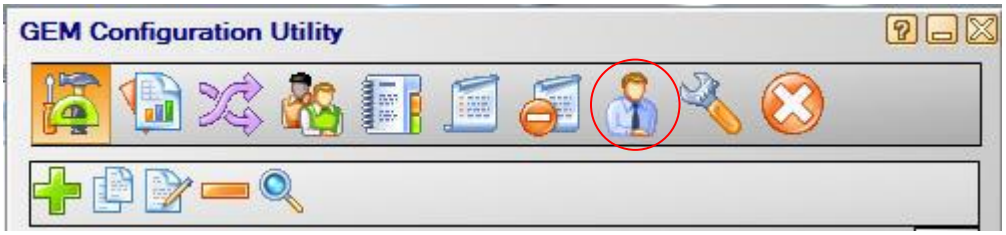
simply set up the first rule in GEM to look for the term in the subject line and if present, ignore the email (i.e., do not capture).

4. Discuss and agree on the initial set of Rules. I would keep this as simple as possible. A good tip is to link them to the agreed security classifications. So, if you agree on say 6 security classifications then begin with 6 Rules, one for each security classification. That is (in the example above) one Rule for Directors, one Rule for sales, etc. You can always add and refine rules as you gain experience but I am a big advocate of "getting wet slowly". Get a simple easy to test and easy to verify version up and running first. You may just select one security group for the initial implementation as a proof of concept.
5. Configure your Rules.
6. Add a 'catch-all' rule as the last rule in GEM (so you can see what your other rules have missed).
7. Test

The most important thing to know about rules in GEM?

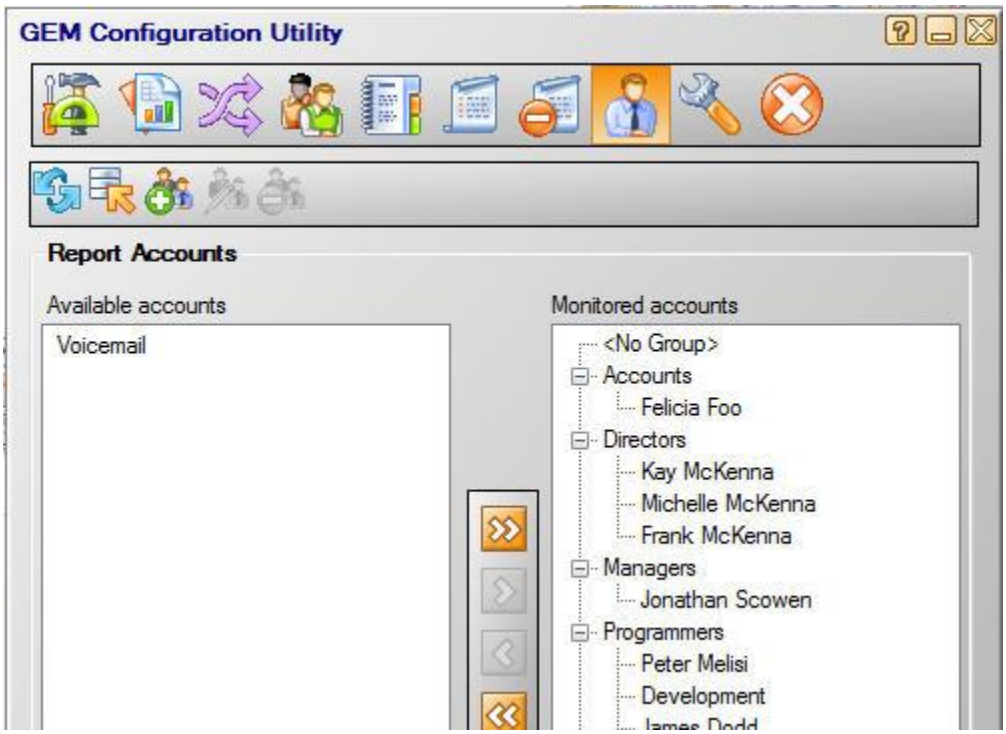
They are applied in order. So the order of your rules is VERY important. When GEM looks at an email it first applies rule 1, the one at the top of your rules list. If that rule doesn't apply it will then look at rule 2 and so on. Always keep this in mind when configuring and 'ordering' rules.

Configuring rules in GEM – where do you begin?



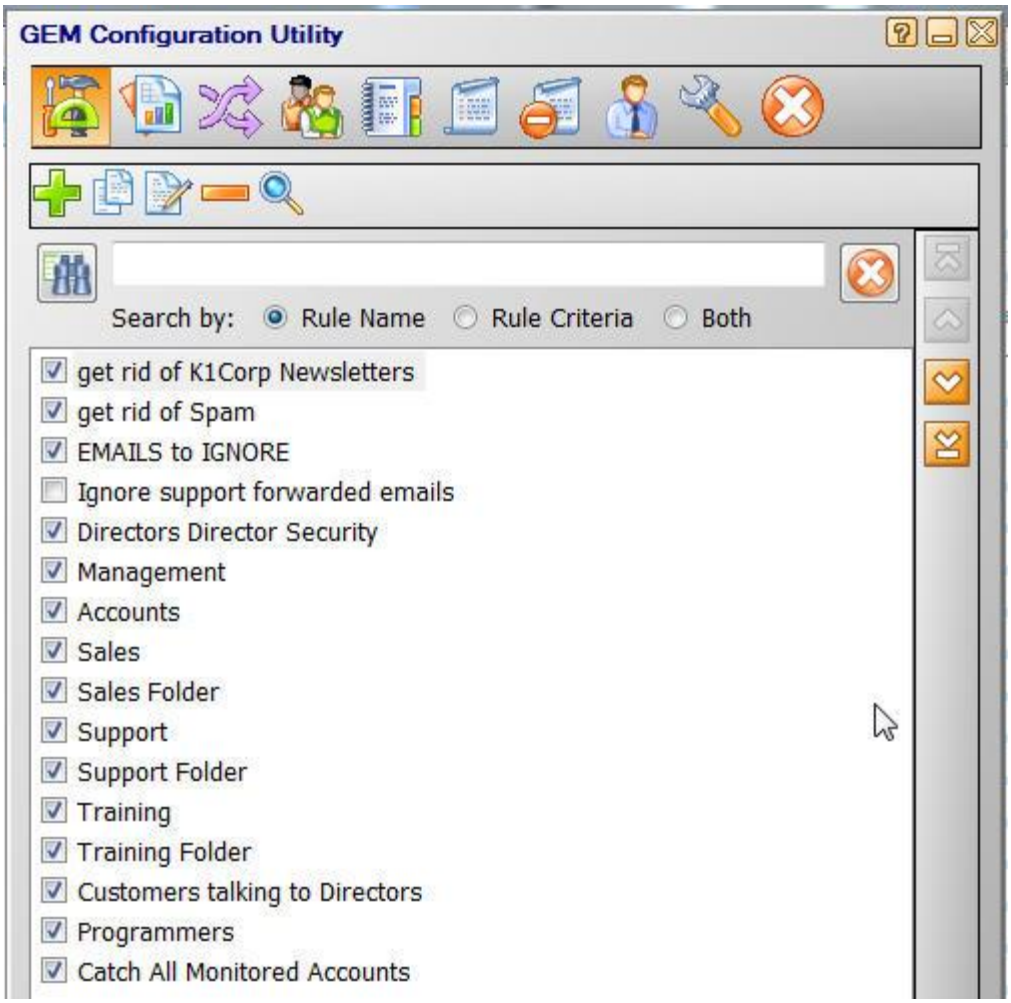
As this example is based around the employee rule and 'group' rules we will begin with the User Configuration icon.

The following user configuration screen is a simple example showing how we have grouped our employees into groups defined by our company security scheme. GEM will automatically populate the left side of this screen when you select your email server. All you have to do is add the Groups (e.g., Accounts or Directors) and then move the employees from the left side of the screen to the appropriate group on the right side of the screen. Now you have what GEM calls 'Monitored Accounts'.



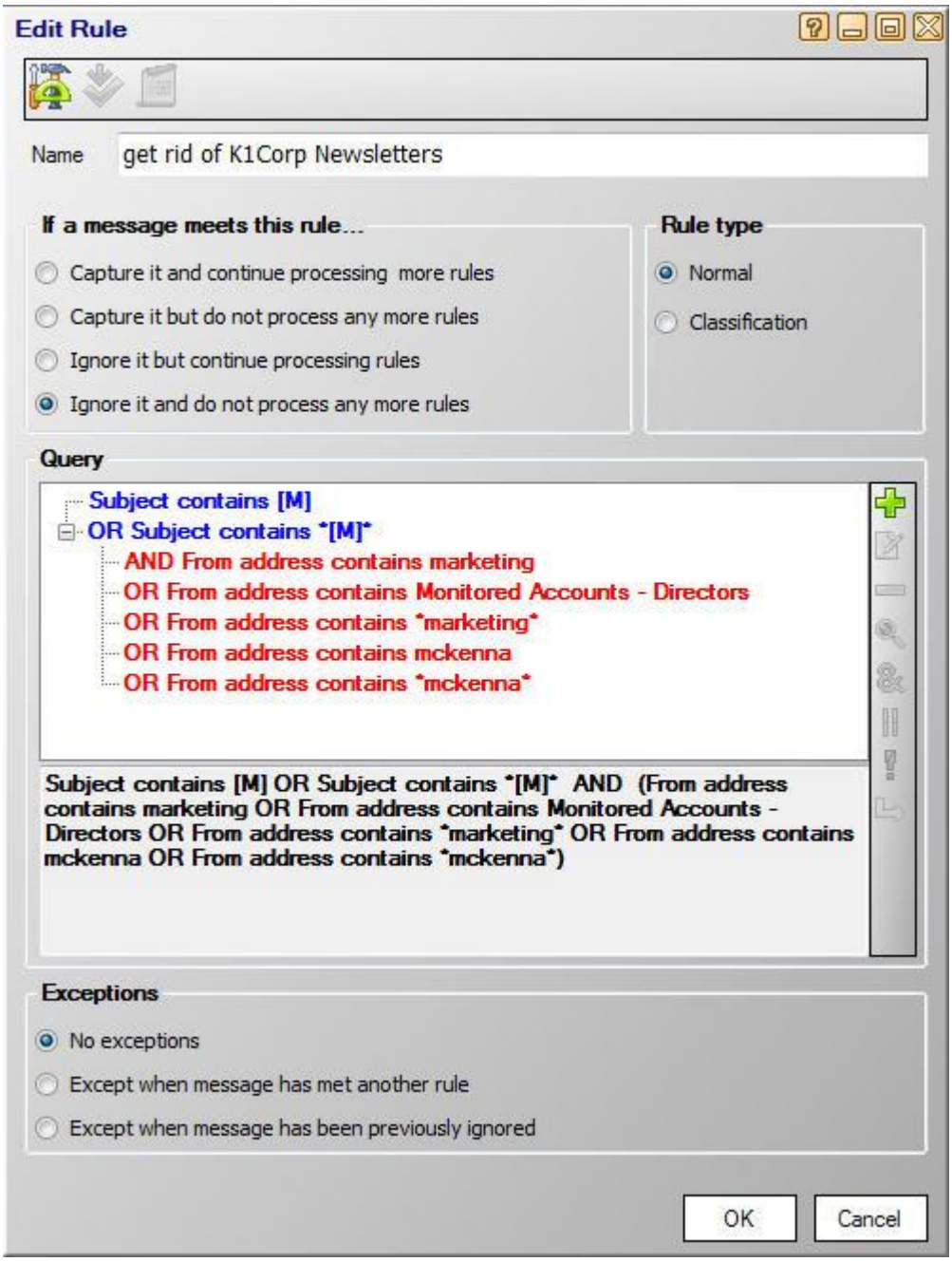
The number of groups you define will determine the number of rules you need to define.

Now let's look at the sample rules screen.



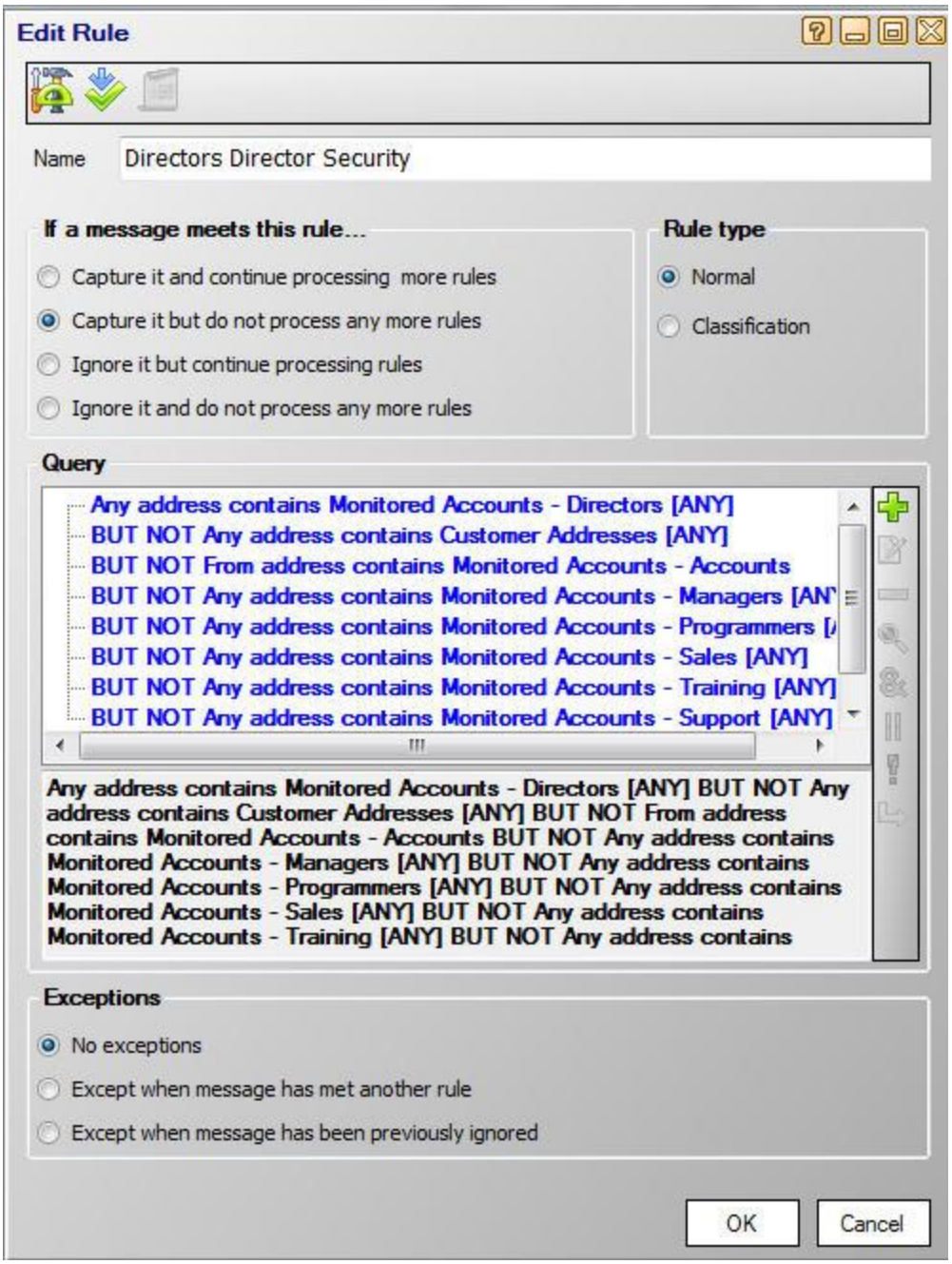
In the above rules screen we have defined 16 rules to manage all of our emails, both incoming and outgoing. Most are based on our employee groups, one is to remove spam tagged by our spam filter and one is a 'catch-all' to make sure nothing falls through our net.

Remember that the rules are processed in order, top to bottom. So, the first thing we do is inspect the email to see if it is one of our marketing emails If it is, we ignore it because we do not want to save it in our RecFind 6 database (we already have a master copy). Then we do the same thing with anything identified as spam.



Notice that we don't set any capture conditions because if this rule is 'true' we are not interested in capturing the email.

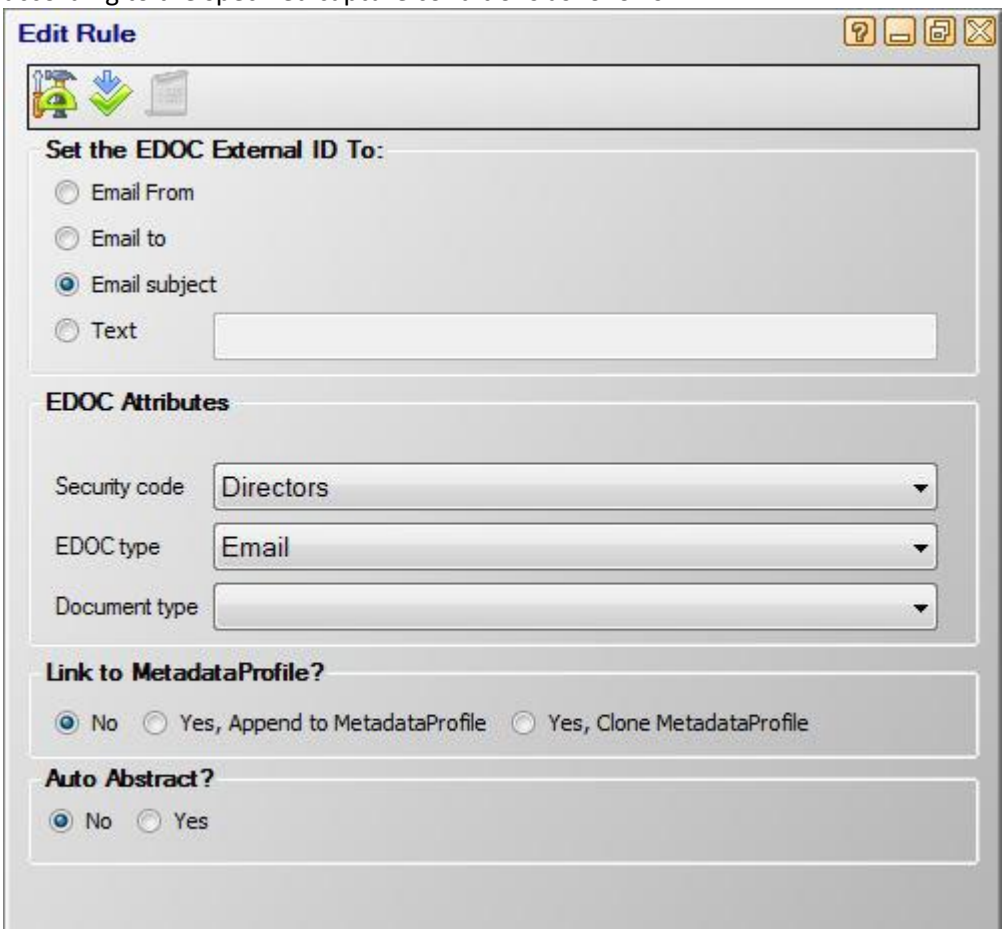
The next rule is the Directors rule.



Notice that with this rule we do set capture conditions (next screen).

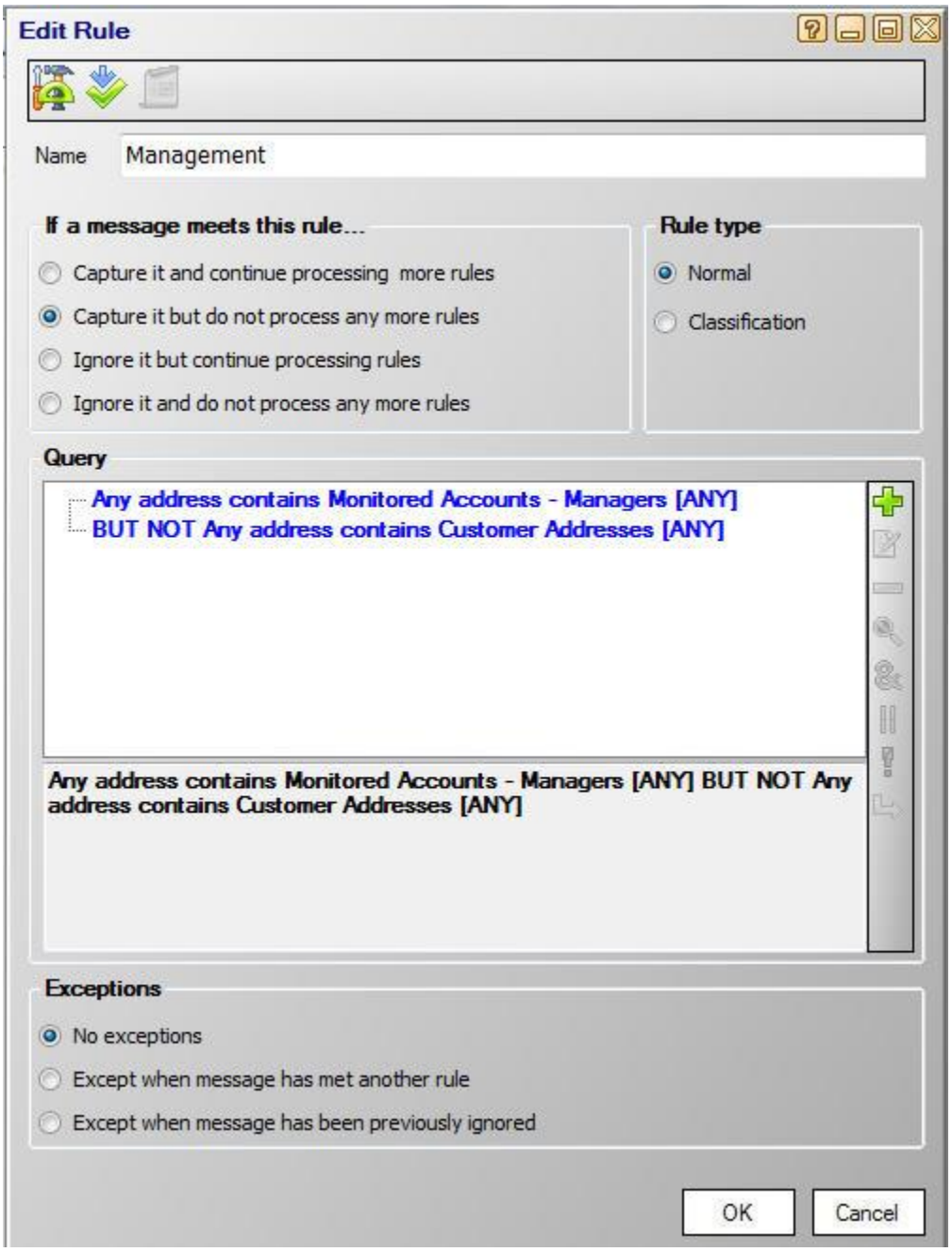
This is a more complex rule because we only want to apply a security code of 'Directors' if the email is from a director to a director or from an external contact to a director or from a director to an external contact. We do not wish to apply the directors' security code to emails between directors and other staff members because that would prohibit those same staff members from seeing 'their' emails once they are stored in the K1 or RecFind 6 database.

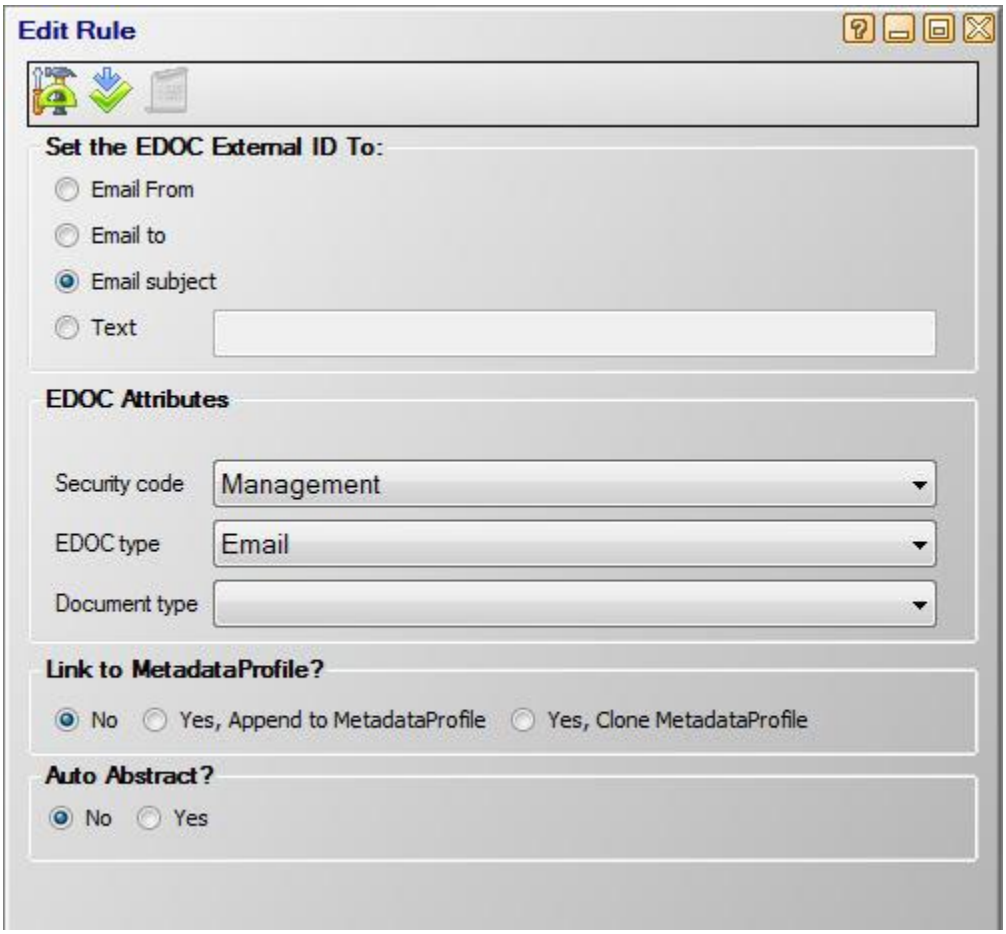
If the email being examined meets this rule we capture it and store it in the RecFind 6 or K1 database according to the specified capture conditions as follows:



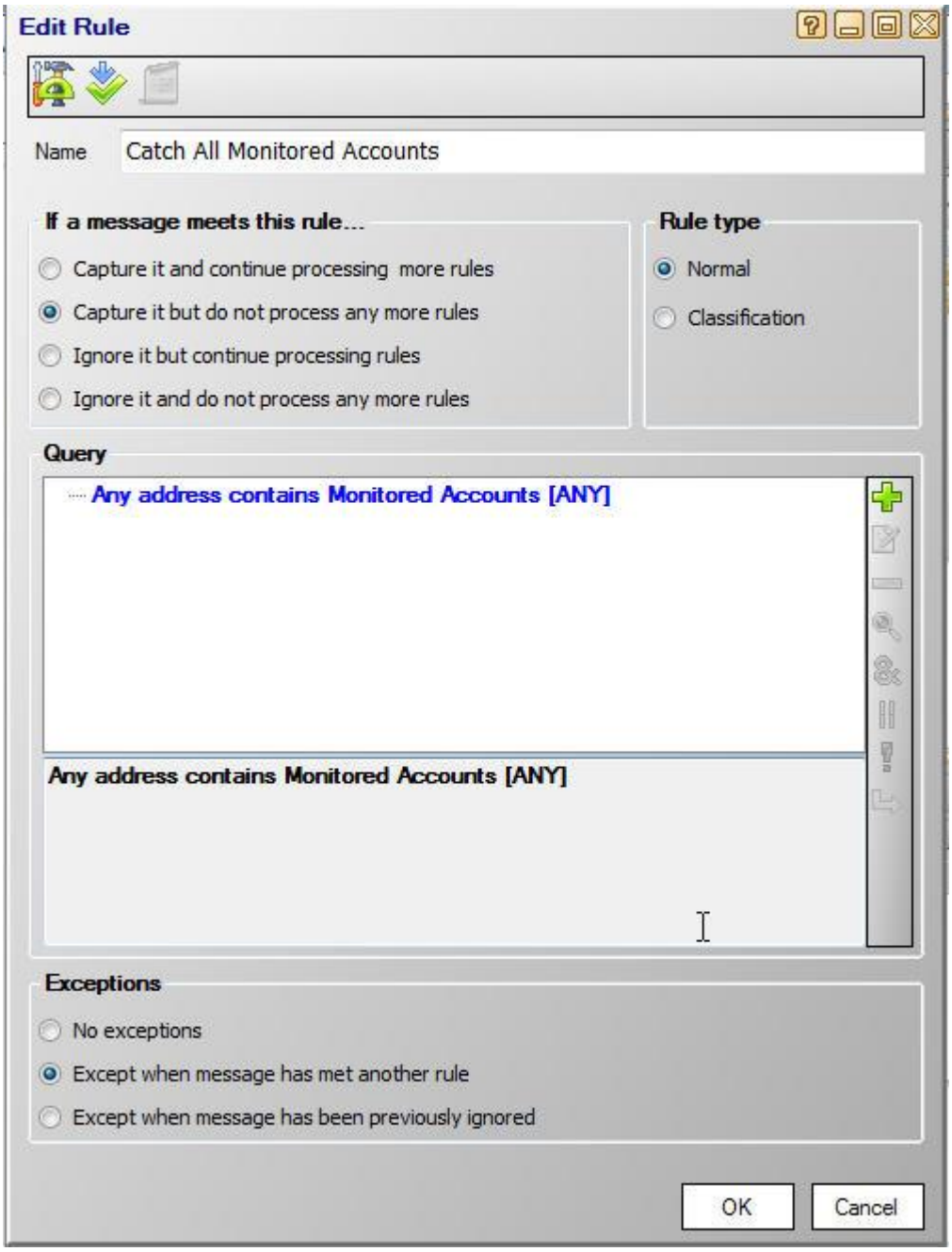
I won't go through all the options and parameters in this paper because they are all covered in the help screens.

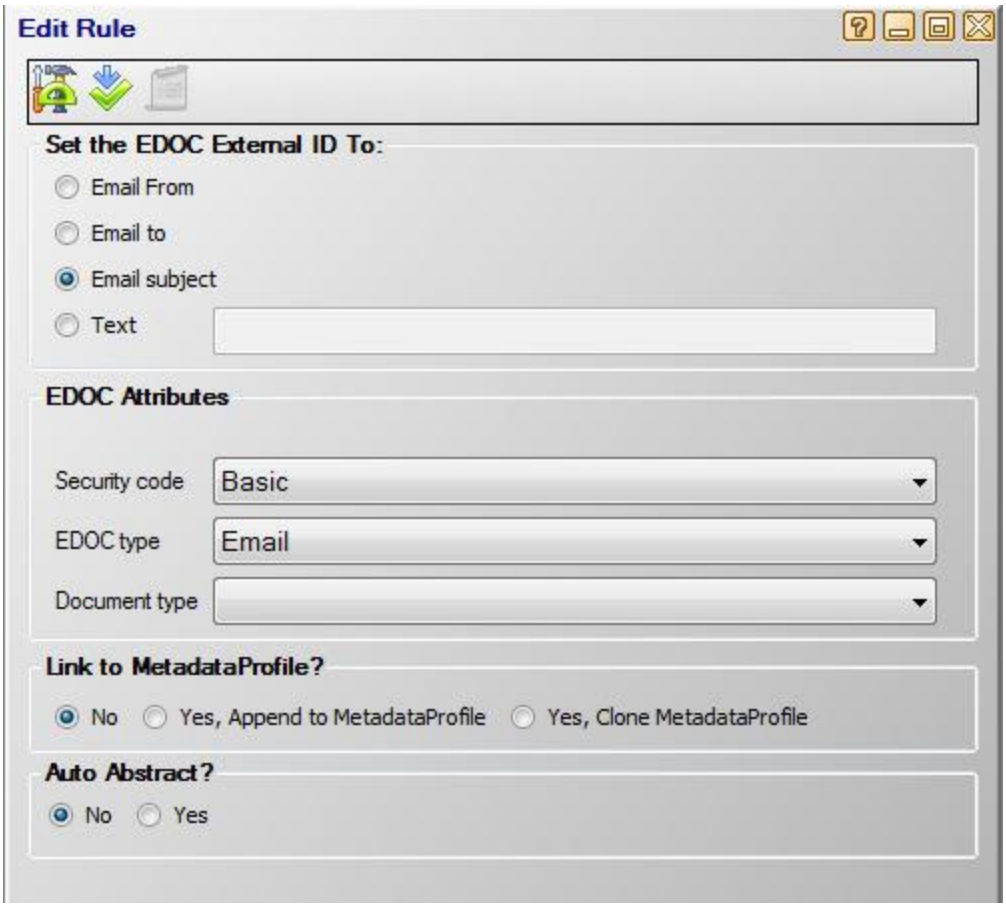
Let's also look at the managers' rule – that rule based on the managers' security code and grouped as a monitored account called 'managers'.


Edit Rule
Name
Management
If a message meets this rule...
Capture it and continue processing more rules
Capture it but do not process any more rules
Ignore it but continue processing rules
Ignore it and do not process any more rules
Rule type
Normal
Classification
Query
Any address contains Monitored Accounts - Managers [ANY]
BUT NOT Any address contains Customer Addresses [ANY]
Any address contains Monitored Accounts - Managers [ANY] BUT NOT Any address contains Customer Addresses [ANY]
Exceptions
No exceptions
Except when message has met another rule
Except when message has been previously ignored
OK
Cancel



And finally let's look at our catch-all rule; making sure nothing slips through our net. This is the last rule to be processed so if an email has conditions that are not met by any of the previous rules it will end up being processed by this last rule.


Edit Rule
Name
Catch All Monitored Accounts
If a message meets this rule...
Capture it and continue processing more rules
Capture it but do not process any more rules
Ignore it but continue processing rules
Ignore it and do not process any more rules
Rule type
Normal
Classification
Query
Any address contains Monitored Accounts [ANY]
Any address contains Monitored Accounts [ANY]
Exceptions
No exceptions
Except when message has met another rule
Except when message has been previously ignored
OK
Cancel



Remember that 'monitored accounts' are those groups of employees we previously defined based on the security used within our organization.

Summary

As a rule of thumb every email we receive or send will have one of our valid email addresses as a sender or recipient (or CC address). So if we use the employee rule we can easily capture all emails sent and received by our organization.

If you have non-specific employee email addresses like say sales@knowledgeonecorp.com or support@knowledgeonecorp.com then you may need to add a rule for each of these.

But, the total number of rules to configure and maintain should still be very small and easily manageable.

The rules engine in GEM is very powerful and allows you to build either simple or very sophisticated BOOLEAN rules based on any attribute of the email. You are therefore able to build a rule to cover almost any requirement.

Most importantly, the rules allow you to emulate exactly what a skilled, experienced human email classifier would do if manually inspecting emails and deciding if and how to capture and classify them.

The real difference being that GEM will repeat the cogitative process infinitely faster and infinitely more consistently than any human classifier.

So, why aren't you using GEM?