Documentation v2.4 (what’s new?)

Mediatrix v2.4

ENTERPRISE INPUT & RESPONSE MANAGEMENT

Powered by Intelligence

Author	ITyX Solutions
Last Change	2015-01-12

Inhaltsverzeichnis

1 Team Management (Mediatrix)

Location	Administration → Team Management Statistics → Agency Monitoring
Neccessary Rights	Projects → <name> → Teammanagement → .*

Team Management/Provider Operations (Agentursteuerung) is an Extension of Mediatrix, which is used to distribute the processes dynamically amongst Agent Groups. Agent Groups are formed by grouping the Agents, either process wise or Location wise, etc.

This feature does not disturb the routing model defined by the core system. It comes into picture just before the routing takes place, to execute the assignment to Agencies. The work on these assignments is done in accordance to the routing model defined.

1.1 Installation Steps

The following Jar file should be pasted in the Mediatrix Installation Directory under **libs/Clientlibs**

mediatrix-agentursteuerung-2.2.1-SNAPSHOT.jar

After pasting the Jar in the Clientlibs, please run a Mediatrix Update. Paste the following in to Mediatrix properties file – at the end of the file.

Open the Mediatrix properties file

Paste the following and save the same

```
#
# TeamManagement
#
# Toggles the menu item "agencies" on or off
# DEFAULT: 1;
teammanagement.frame=1
# Specifies in which extra-column the Agency information is written.
# DEFAULT: 0 - No information is stored.
teammanagement.mailinbox.column=1
micolumn.1=assigned to
# Specifies in which extra-column the Agency information is written. Last
Assignment.
# DEFAULT: 0
teammanagement.mailinbox.lastassignment.column=1
# Which routing model is to be used as the default
# DEFAULT: 1 (Prozentrouting)
teammanagement.defaultrouting=1
# Can a MX-user be assigned to more than one agency
```

```
# 1 = true ; 0 = false
teammanagement.agent.multipleTeams=0
# Interval of the update within the monitoring (indication in minutes)
teammanagement.monitoring.intervall=5
# Interval of the update for the interval monitoring
# allowed Input: 15,30,45,60
# DEFAULT: 15 Minutes
teammanagement.monitoring.intervalmonitoring.interval=15
# Deletes data older than X days (in days)
# DEFAULT: 0 off
teammanagement.monitoring.intervalmonitoring.maxAge=2
# Sets the color (RGB) of the highlighted columns in aging monitoring
# DEFAULT: 153,204,255
teammanagement.monitoring.agingmonitoring.highlight.column.rgb=153,204,255
# Allows displaying of the Operators re-submissions
# DEFAULT: 0
# 1 = true ; 0 = false
teammanagement.personalrequeue=1
# Once activated, all tabs are loaded at startup. If disabled, the switching
process, the active tab is loaded.
# DEFAULT: 0
# 1 = true ; 0 = false
# teammanagement.monitoring.tabs=0
# Specifies whether the monitoring window can be started multiple times.
# DEFAULT: 0
# 1 = true ; 0 = false
# teammanagement.monitoring.multiInstanz=0 (commented out for the moment)
```

Import the following business rules into the corresponding project and then activate the same.

- AgentursteuerungAntwortAnzeigenRule.rul
- AgentursteuerungClientObjectsControlRule.rul
- AgentursteuerungFrageAntwortAnzeigenRule.rul
- AgentursteuerungFrageAnzeigenRule.rul
- AgentursteuerungMailInboxRule.rul
- AgentursteuerungServerSystemRule.rul
- IServerMonitorRule.rul

The following routing services must be saved as follows:

- ityx-agentur-routing.conf : ID/Conf/Service
- 22_ityxagenturrouting : ID/bin

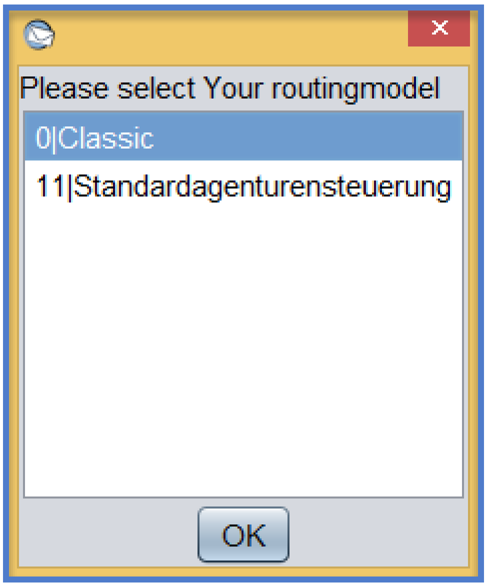
Restart all the Services and Application again.

1.2 Rights to Team Management

1.2.1 Agent

Any agent assigned to an Agency/Team, automatically gets the rights to access the Team management mails in the Operator Mode. No special assignments of rights is required for the same.

An Agent is asked to select a routing model on logging into the Application, if he or she is a part of a Team/Agency.



On selecting the **11|Standardagenturensteuerung** Routing model, the mails assigned by the Admin to the different agencies are respectively available for processing in the operator mode.

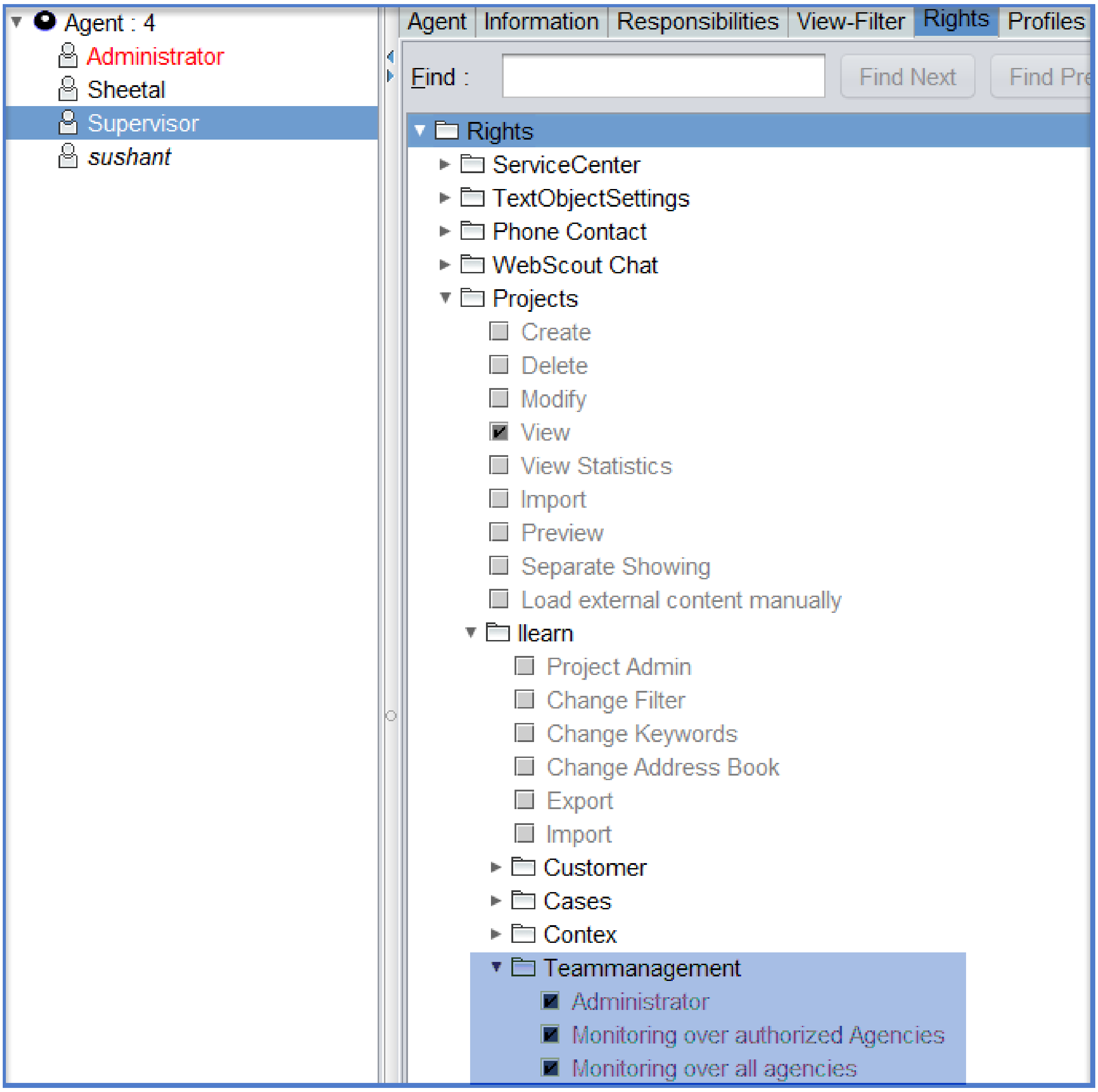
1.2.2 Administration Rights

An Agent who is already an Administrator, will automatically have the rights to Team Management assigned, if the extension is configured for the customer.

But for an Agent who is not a Project Administrator, needs to have Team Management rights assigned explicitly in order to work as an Administrator for that Agency/Team.

These rights maybe assigned as follows:

Administration → Agent → Edit → Select Project → Show → Project → Select Project → Team Management rights



1.2.2.1 Team management →Administrator

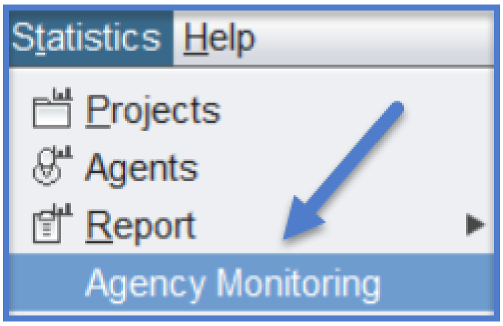
Assigns the administrative rights for the team management.

Admin can see all the mails assigned to the different teams and also manually assign mails to different teams if required.

Note**: Mediatrix-Administrators and Project administrators have this right automatically assigned, it need not be assigned separately. The administration of the team management extension is possible over **Administration→Team Management/Provider Operations (new Window)** or over **Administration→Project→Edit→Team Management/Provider Operations (embedded window).

1.2.2.2 Team Management →monitoring all the agents

This right issues the possibility to invoke/check the Agent-Real time-Monitoring, which can be called over the **Statistics→Agent Monitoring** within the Mediatrix-Clients. Any desired team can be monitored using this.



1.2.2.3 Team Management → Monitoring the authorized Agents

This has the same effect like Team Management→monitoring all the agents, only with the limitation that this filter allows the monitoring of only those sub-projects for which the Administrator/Agent holds responsibilities.

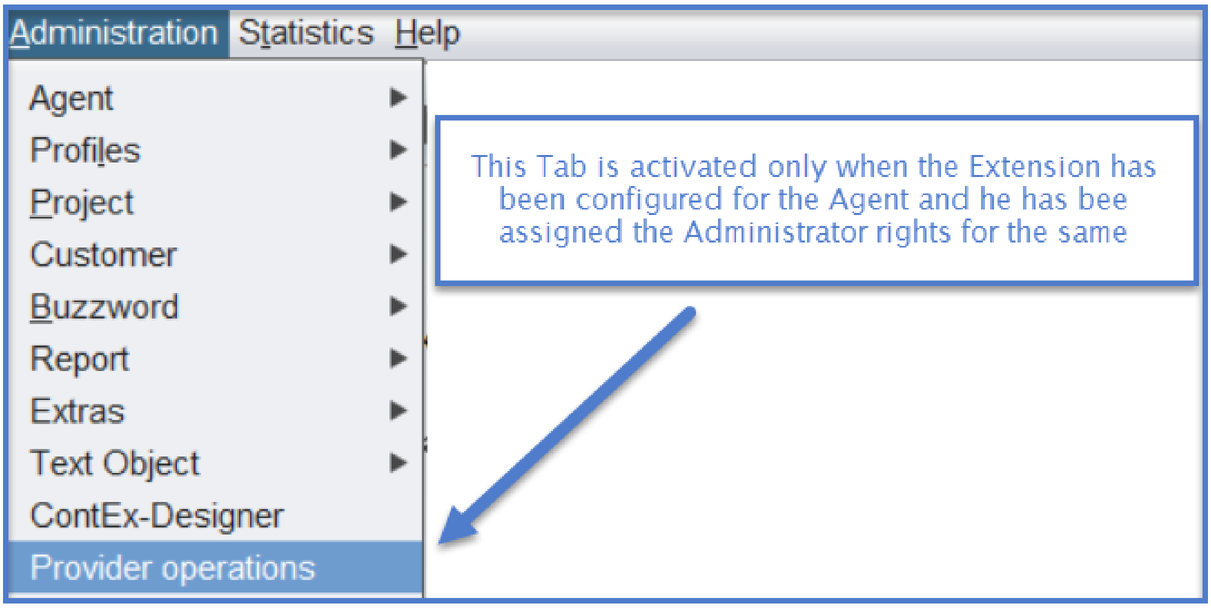
***Note:** A Mediatrix Administrator or an Agent with the Team Management rights assigned will see the Team Management/Provider Operations Extension configured in his Application. The Admin/Authorized agent can now configure an Agency/Team and assign Agents to the same and also configure the Routing.*

1.3 Agency/Team Configuration

The Agent with Team Management rights assigned or a Mediatrix Administrator can configure the Agency/Team.

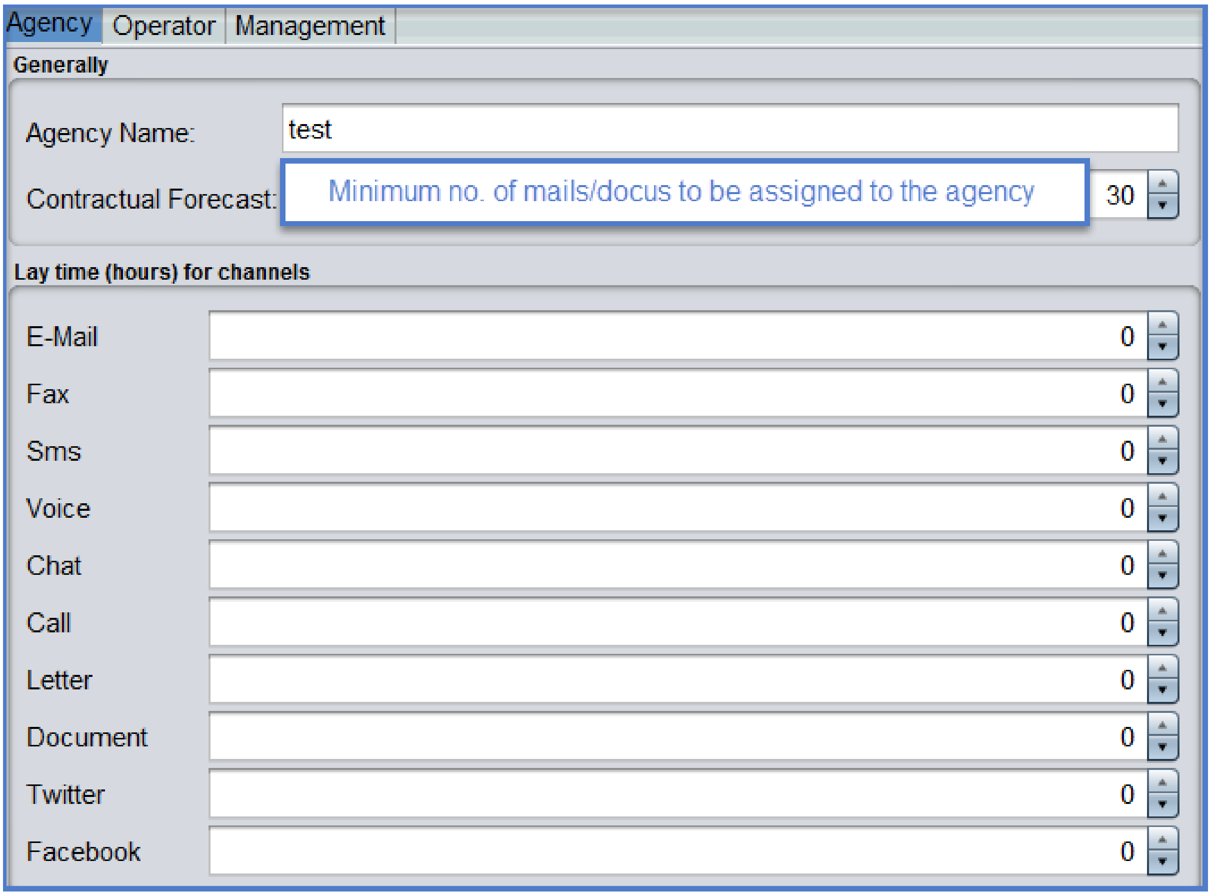
This can be configured as follows:

Administration → Team Management / Provider Operations



1.3.1 Agency

After clicking on the Provider Operations/Team Management tab above, the Admin can configure the Agency, assign Agents to the Agency and assign the Subprojects for which the agency will be responsible.



- **Agency Name:** A name needs to be assigned to the group of Agents.
- **Contractual Forecast:** Minimum number of mails or documents to be processed each day by the Agency is mentioned here.
- **Lay time (hours) for channels:** Maximum idle time for each channel can be mentioned here. But it should be set in accordance to the SLA. This value is entered in the calculation of the Service level routing for the Agencies. If this time is exceeded on the previous day, it will have a negative effect on the routing to the Agency the next day.

1.3.2 Operator

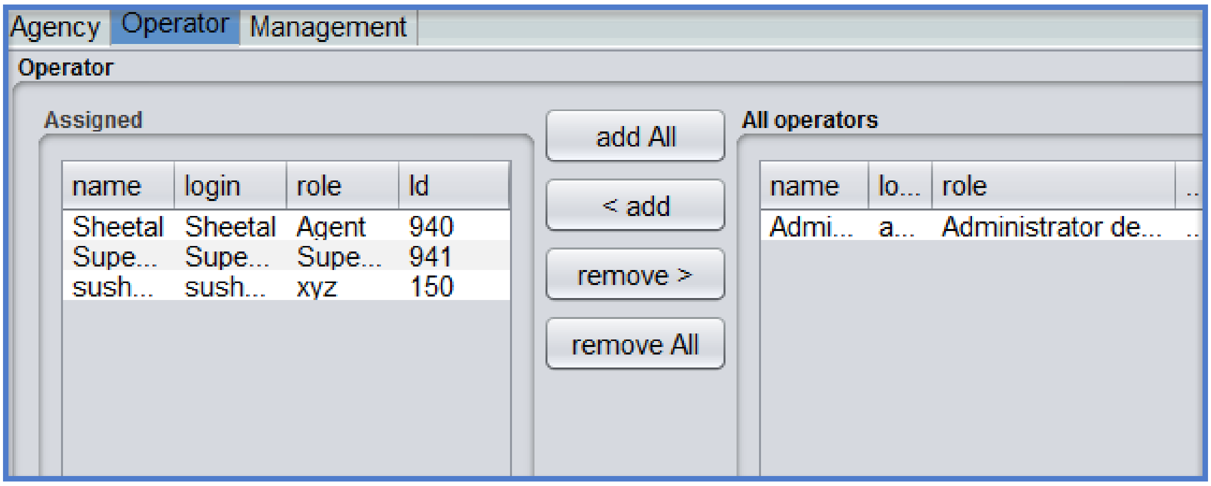
Here the Agent[1] assignment to the Agency created will take place.

After the Operator Tab is clicked on, you may simply click on the **ADD** button to assign the Agents to the Agency created.

The **REMOVE** button deletes the Agent assignment with the Agency.

[1] If the Administrator is assigned to an Agency, he/she will no more able to view the mails in the mailbox or do the manual assignment of mails to the Agencies.

The **add ALL** and **remove ALL** button adds all the Agents to the Agency and deletes all the Agents from the Agency respectively.



1.3.3 Management

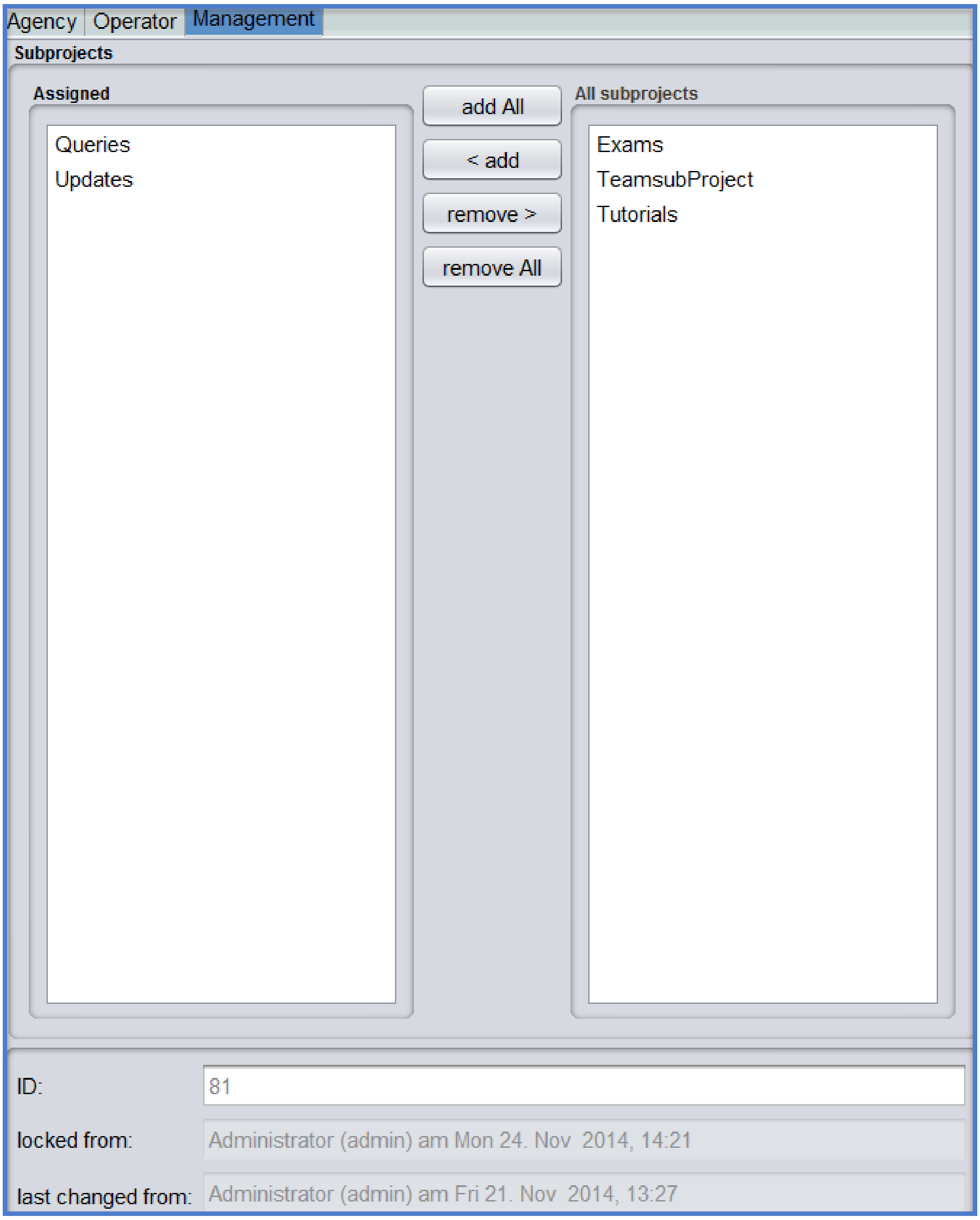
Agency created to be assigned to the respective Subprojects here.

As in case of the Operator Tab, the management tab also offers the **ADD** button to assign the subprojects to the Agency created.

The **REMOVE** button maybe used to un- assign a Subproject from the Agency.

The **add ALL** and **remove ALL** button adds all the Subprojects to the Agency and deletes all the Subprojects from the Agency respectively.

The fields **ID**, **locked from** and **last changed from** get populated automatically.



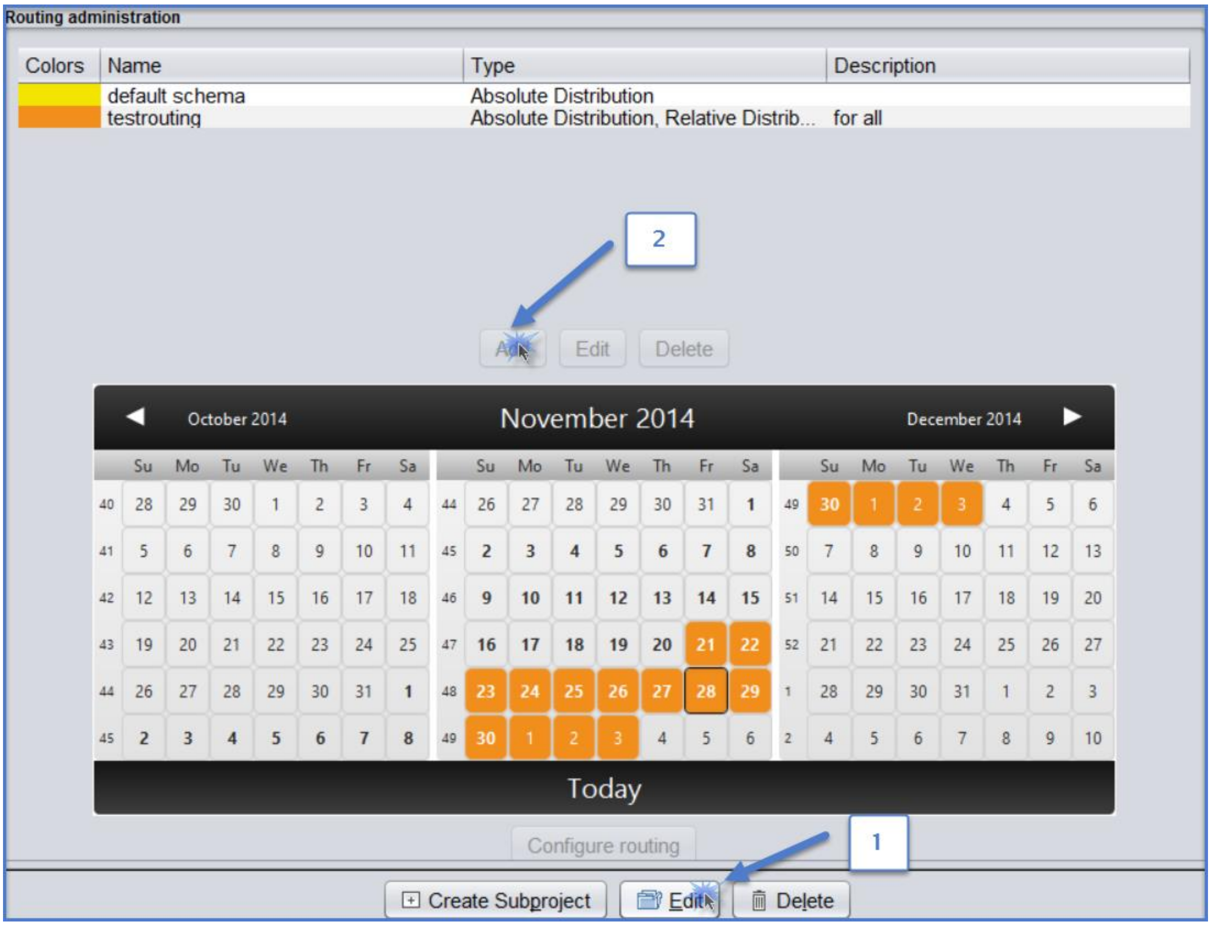
1.4 Scheme definition and Routing

After configuring agencies/teams. It is necessary to define a routing mechanism to manage distribution of mails/documents to these agencies/teams. Hence a Scheme Definition is necessary.

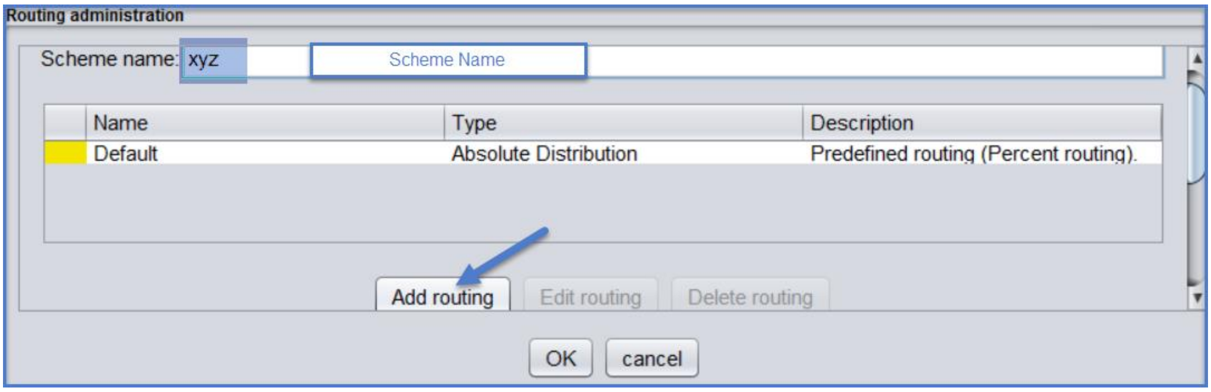
A Scheme may be defined as a group of different routing models configured to manage the mail/document distribution for an Agency/Team.

Administration → Project → Edit → Select a project → Team Management /Provider operations → 1 Edit → 2 Add → Give a name for the Scheme → OK

After clicking on the **ADD** button, you can define a Scheme under which different routing models may be defined.



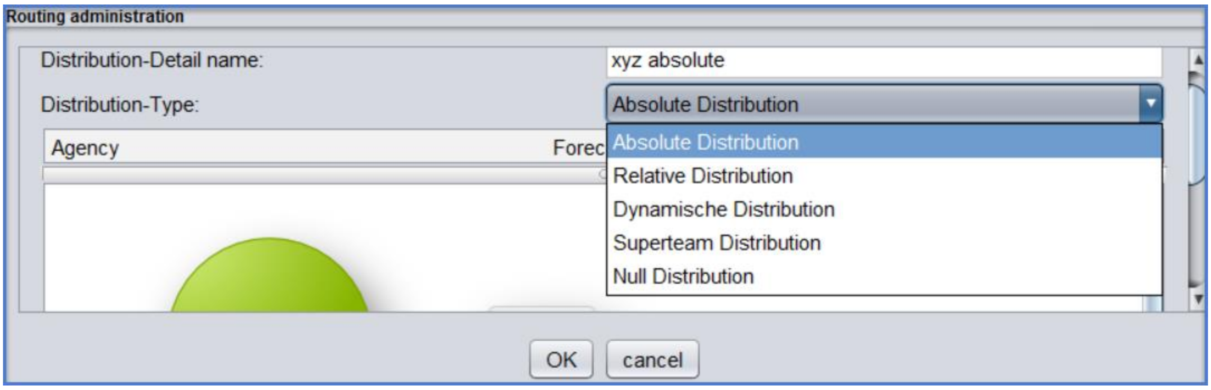
Enter a name for the new Scheme and click on **Add Routing**.

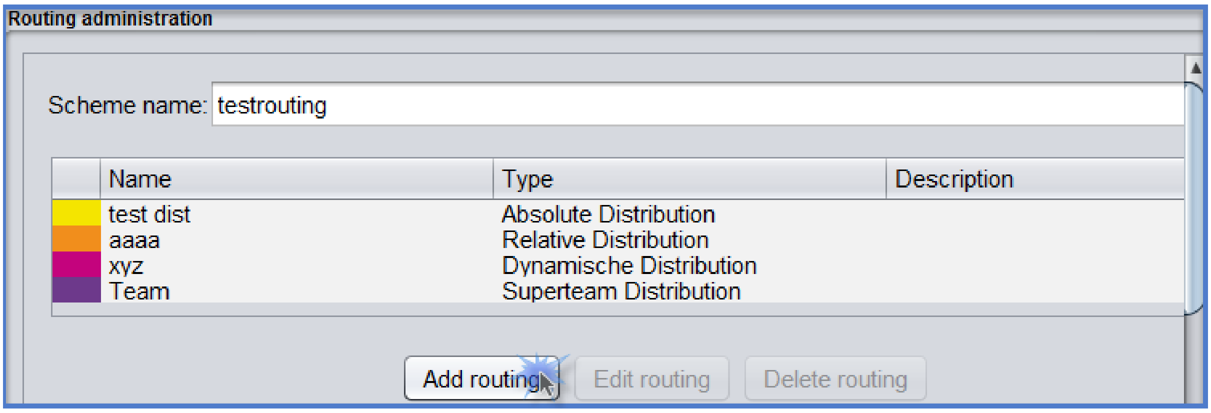


Enter a name for the distribution in the **Distribution-Detail name**.

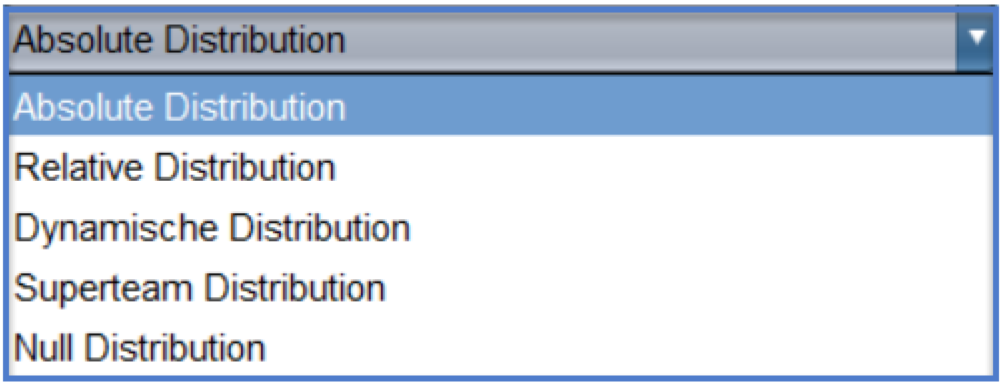
Select the type of **Distribution type** you want to configure and click on **OK**.

The new configured distribution will be displayed to you.



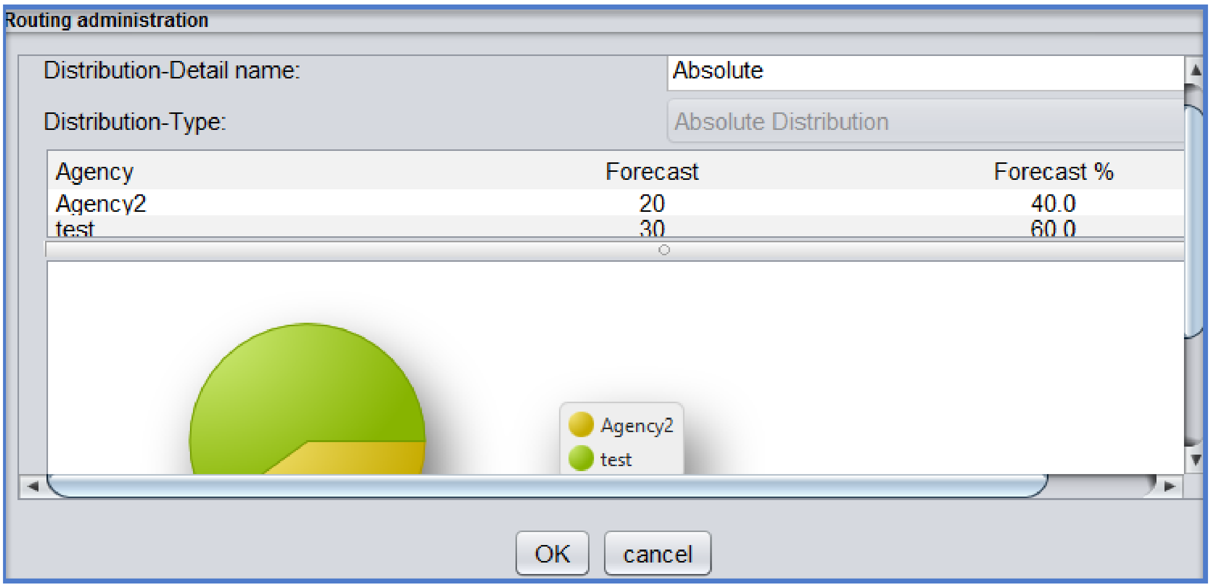


1.5 Types of Distribution available



1.5.1 Absolute Distribution

This distribution is configured in such a manner that the sum of all entries in the Forecast% column is 100. Each Team/Agency is assigned with a certain percent of the total mails/documents coming in for the Subproject. The distribution of work takes place according to the Forecast percentage defined.



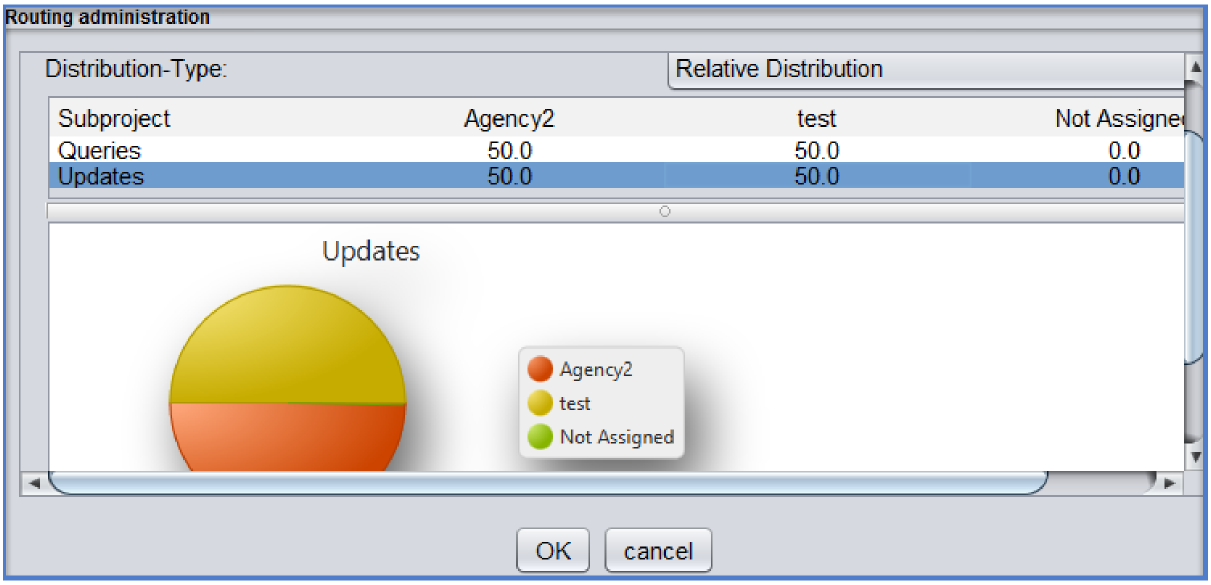
1.5.2 Relative Distribution

This distribution is also a standard variant. Should an explicit routing model not be assigned for a given day, then relative distribution is always used for working. If the number of documents/mails available are more or less, then the teams are distributed the documents as per the percentage mentioned.

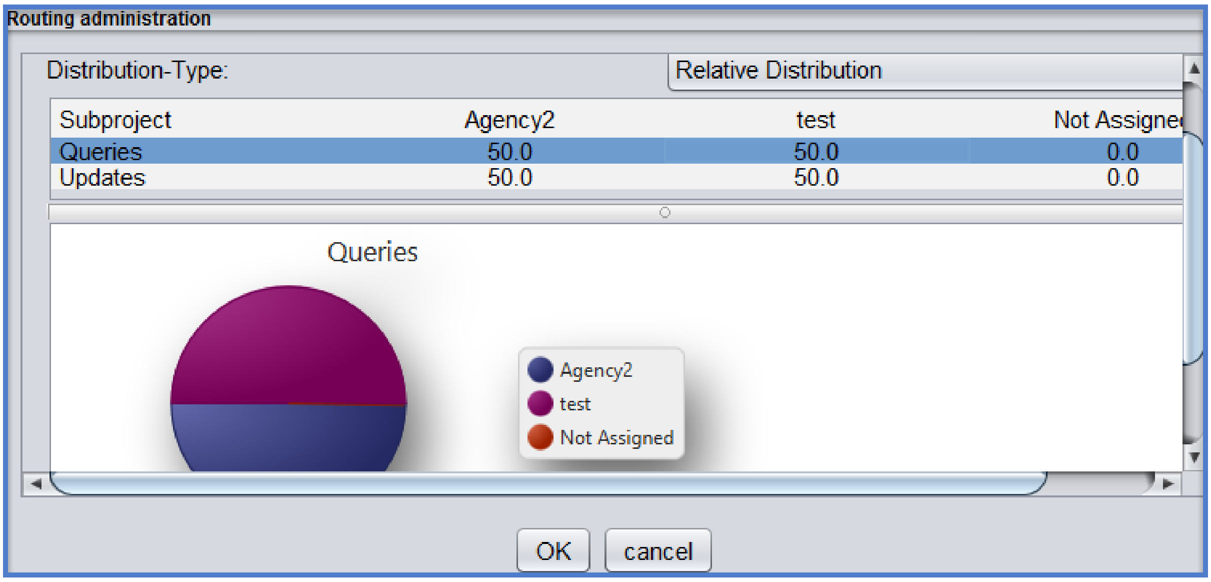
For e.g. when a team TEST has a value of 50 and the team AGENCY2 of 50, then the documents/mails are assigned 50% to the team TEST and 50% to the team AGENCY2.

The distribution is done here Subproject wise.

Subproject Updates

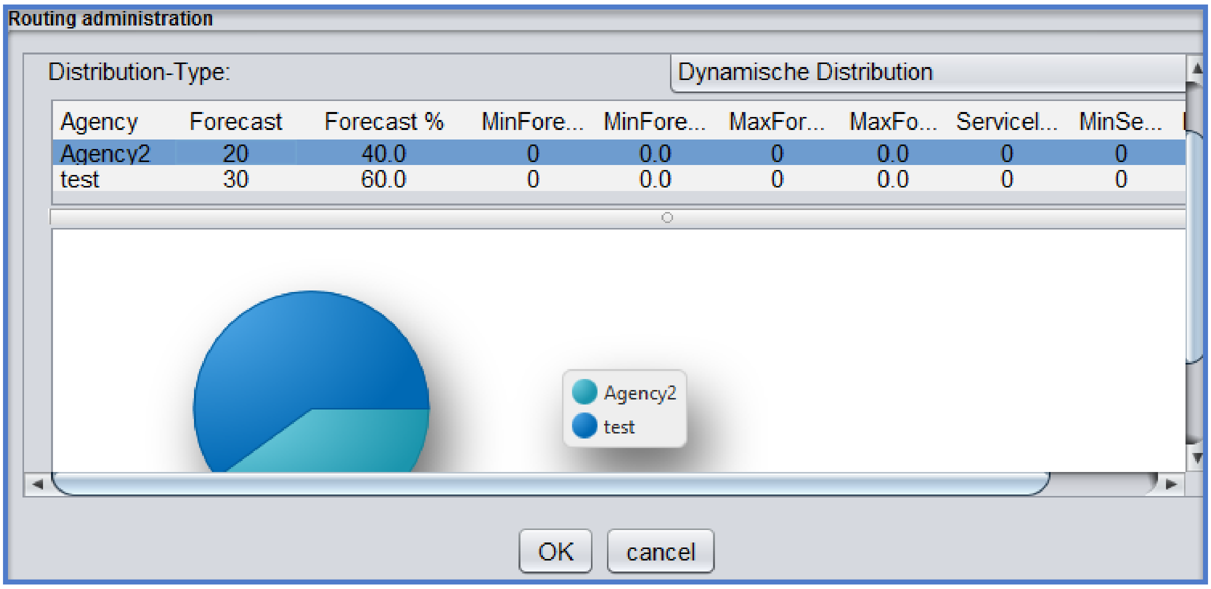


Subproject Queries



1.5.3 Dynamic Distribution

In this form of distribution, Agencies/Teams are provided with the question on a percentage basis. The target value of the 'to be' worked upon documents/mails is setup as „Forecast". Also the Service level can be entered here to mention the maximum and minimum time assigned for working on the assigned documents/Emails. Dynamic Routing facilitates faster working.



Term	Description
Team	Fixed – name of the team. It can be edited over 'Edit team'
Forecast	Editable – The recorded value from the team management setup. It is the count of the documents to be worked upon by a team on a daily basis.
Forecast %	Fixed – One of the 'forecast' calculated percentage count, which reflects the ratio of the distribution between the teams.
MinForecast %	Editable – is the percentage value of the minforecast entry (20 corresponds to 20%).
MinForecast	Fixed – this value is calculated from the values forecast and minforecast%.
MaxForeCast %	Editable – is the percentage value of the maxforecast entry (20 corresponds to 20%).
MaxForeCast	Fixed – this value is calculated from the values forecast and maxforecast%.
Servicelevel	Editable – A service level value can be entered here (value from 1 to 100). However this value has very little impact on the routing model.

MinServicelevel	Editable – Percentage value in the entire data (20 corresponds to 20%).
MaxServiceLevel	Editable – Percentage value in the entire data (20 corresponds to 20%).

1.5.4 Superteam Distribution

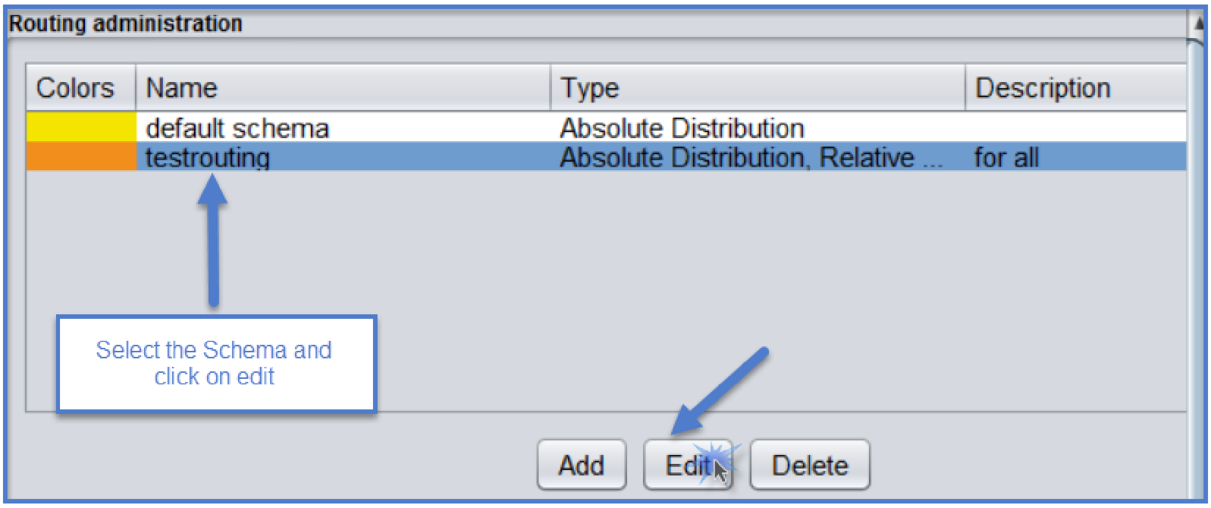
When this form of Distribution is active, all the teams work together as one team and the mails distributed can be seen and processed by every agent of every team.

1.5.5 Null Distribution

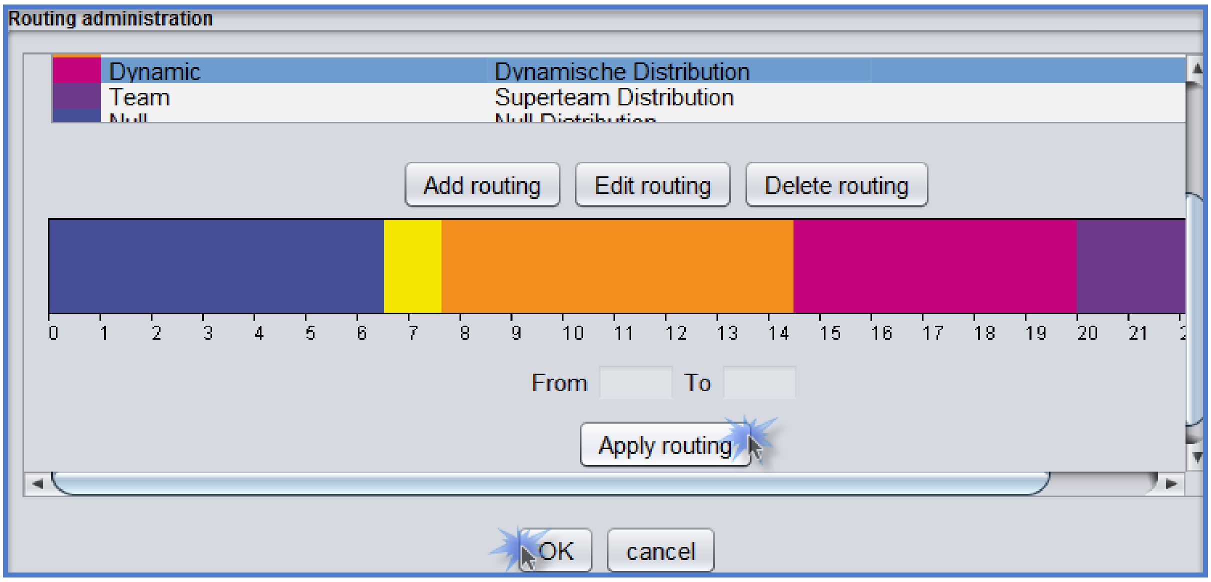
This form of Distribution is activated when no routing of mails should take place to the Teams/Agencies. In such a scenario the default routing configured for Agents will come into function.

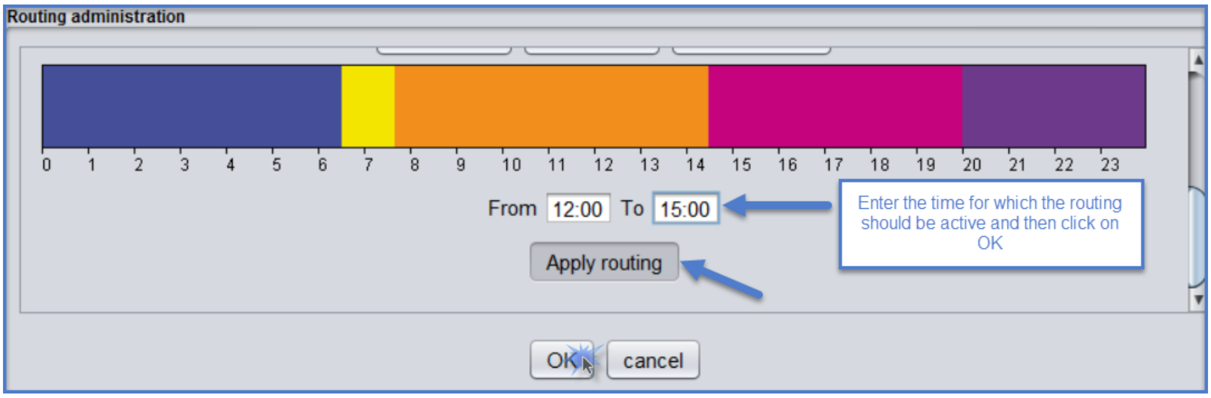
1.6 Applying the Routing Model (Distribution model)

Select the Scheme to be defined and click on Edit to edit the same.



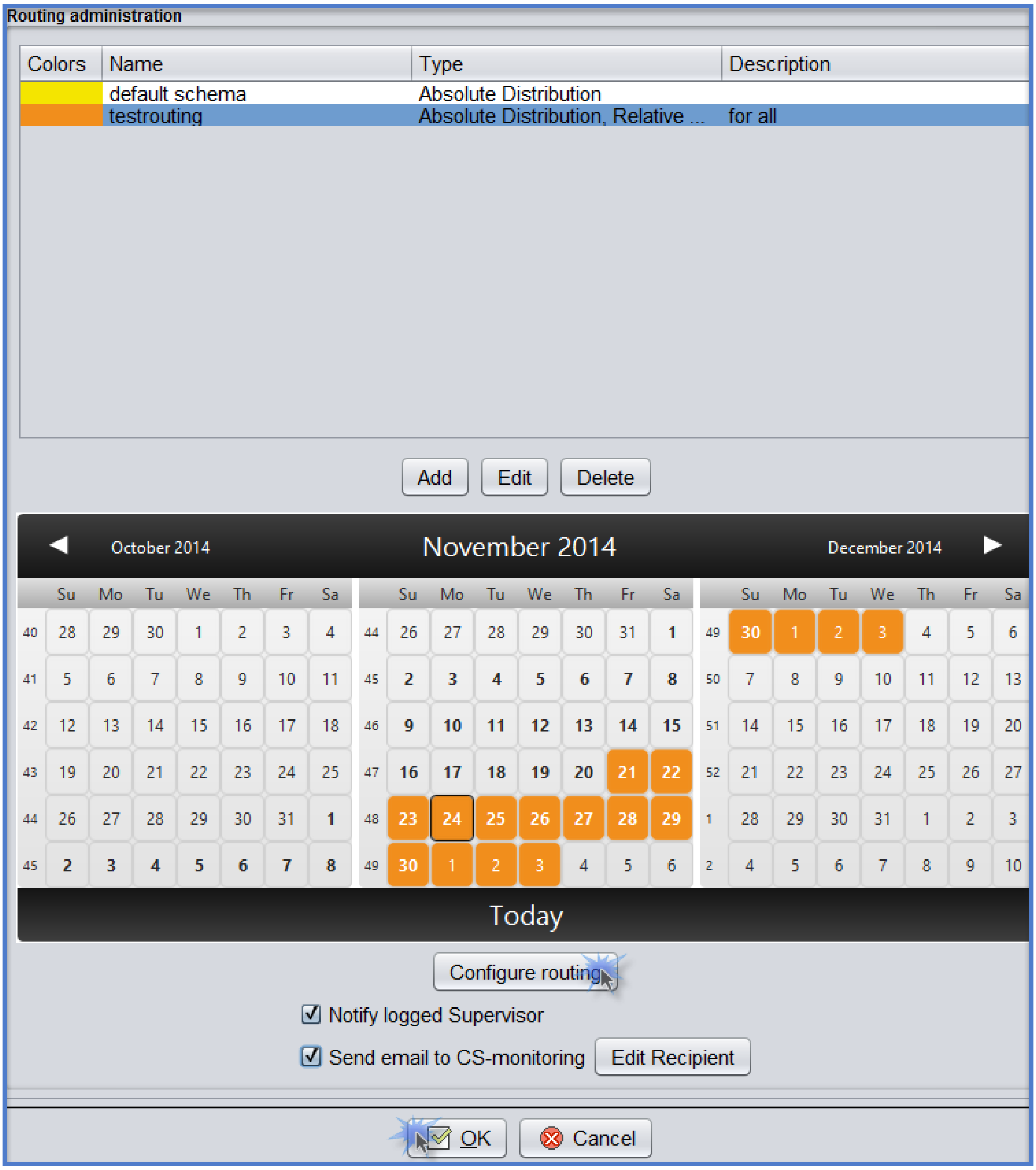
Now select the routing model/distribution model for which the time needs to be defined and click on **Apply Routing**. Thus the timespan for each routing model to be functional maybe defined.





1.7 Configuring the Routing

Once the timings are set, select the **Schema** and click on **Configure Routing** and click on the dates for which this Schema should be valid. Then click on **OK** to save the same. The dates selected will be highlighted in a different colour.

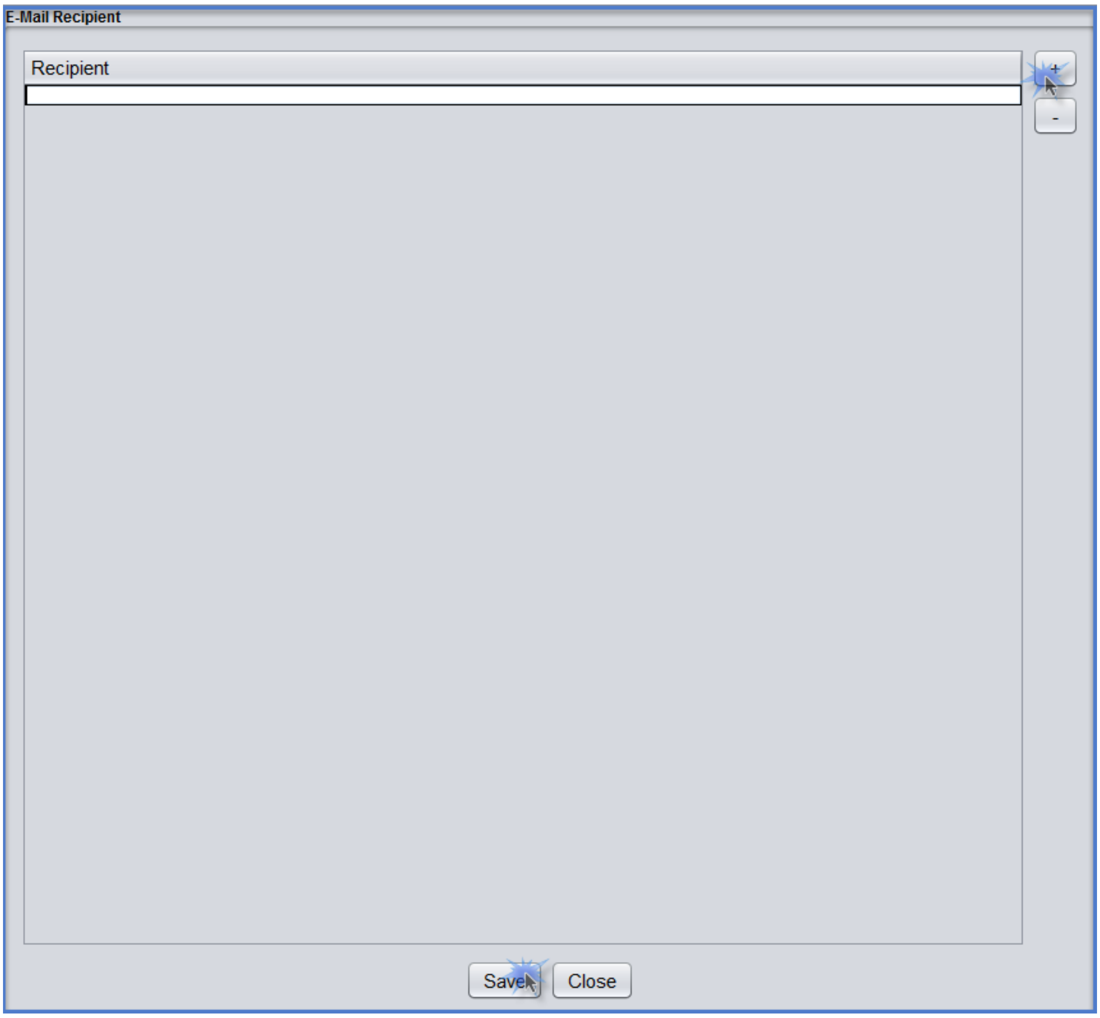

Routing administration
Colors | Name | Type | Description
default schema | Absolute Distribution
testrouting | Absolute Distribution, Relative ... | for all
Add
Edit
Delete
October 2014
November 2014
December 2014
Today
Configure routing
Notify logged Supervisor
Send email to CS-monitoring
Edit Recipient
OK
Cancel

1.7.1 Notify logged Supervisor

If this option is active, then all people who are logged in and have the right Agentursteuerung:Administrator/Team Management:Administrator will be informed/notified via a Mediatrix message (Popup-Window).

1.7.2 Send Email to CS-monitoring

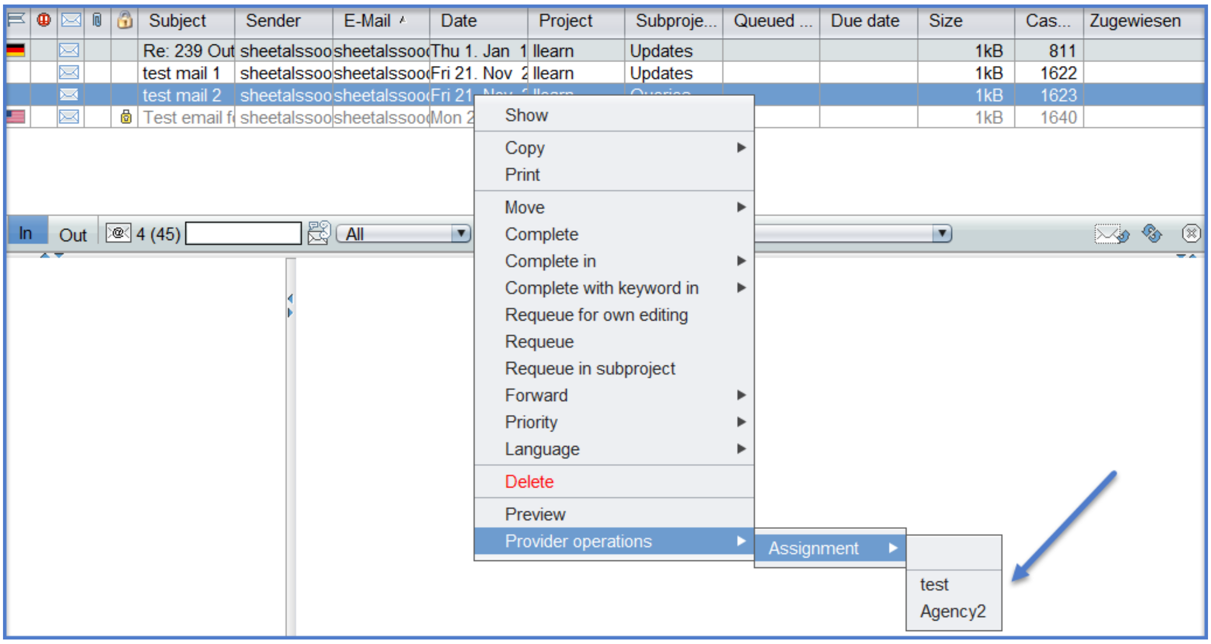
After clicking on this option, we need to enter the email IDs of Administrators/Agents to whom the notification should be sent in case there is a failure with the Routing/Distribution.



1.8 Manual Distribution of Mails

The Administrator has the right to manually assign the mails to the Agencies.

It can be done by simply right clicking on the mails seen in the **Mail-Inbox** and assigning it to the correct Agency for processing.



NOTE*: the routing/distribution model defined for Team management comes into picture, only to get the mails/queries distributed to the respective Teams/Agencies. Once the teams get the mails/queries assigned, the internal distribution to respective agents of the team, happens as per the routing model defined at the Agent level in Mediatrix.*

2 Archiving Mediatrix Data (Mediatrix)

The archive as its name suggests is used to archive the emails in the Mediatrix. It helps in bettering the system performance by keeping the customer histories minimal.

The archive service mentioned below runs in the background continuously and need not be started explicitly by the customer to facilitate archiving.

The Services that run in the background are as follows:

- 17_mediatrix_archive_scheduler
- 17_mediatrix_archive_scheduler.sh (for Linux)

Note*: The Archive Service is set as default for every customer using Mediatrix. In case it is stopped manually by the customer, then the queries regarding the system performance will not be entertained by Support.*

2.1 The Archive Tab

All the completed mails which are more than a year old (365 days) get archived automatically.

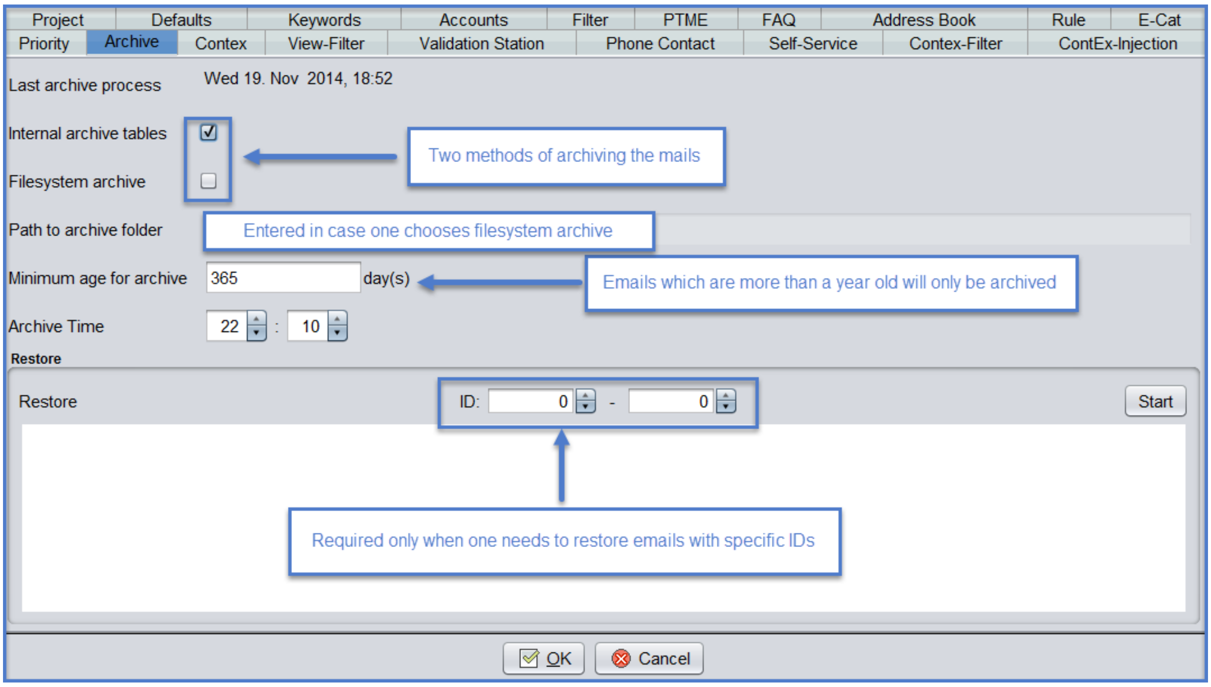
Whenever a new Project is created in Mediatrix, the Archive tab for that Project gets populated with certain default parameters automatically.

Following default parameters get populated in the Archive tab as soon as a new project is created:

- **Internal archive tables** gets checked
- **Minimum age for archive** gets set to 365 (i.e. one year)

You can view the same under:

Administration → Project → Edit → Choose the project to be edited → Archive → Edit

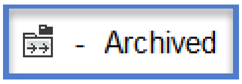


- **Last archive process**: Displays the time when the mails were archived last.
- **Internal archive tables**: This option is checked by default when a project is created. The mails archived will be archived to the internal tables within Mediatrix in this case.
- **Filesystem archive**: If this mode of archiving mails is chosen, then the mails will get archived to the external Filesystem.
- **Path to the Archive folder**: If Filesystem archive is chosen, the path to the Filesystem is required to be mentioned here.
- **Minimum age for archive**: this is by default set to 365 days, i.e. one year.
- **Archive Time**: Here the time is mentioned for the archiving to get executed everyday.

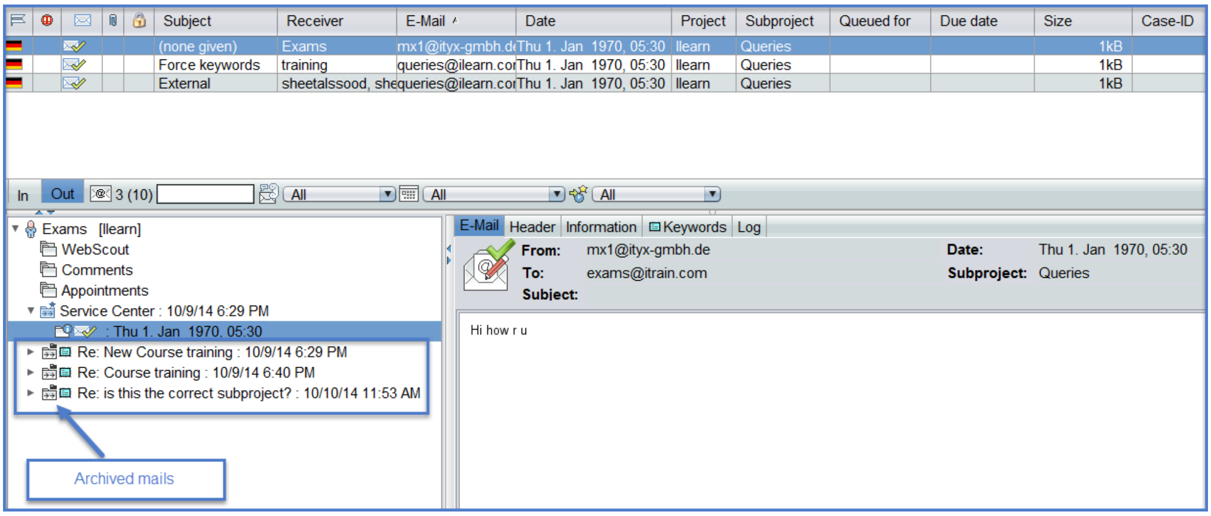
2.2 Archiving of Mails

Mails are archived once every 24 hours, depending on the setup done under the archive tab. Please refer to the Chapter 1.1 for the same. Every time the archive service runs in the background, it checks for completed mails which are more than 365 days old and have not yet been archived. Such mails then get archived.

The mails on getting archived will no more be visible in the mailbox and can be identified with the 'Archived' symbol attached with them as shown below.



Archived mails in the Mailbox:



2.3 Archived Mails Restoration

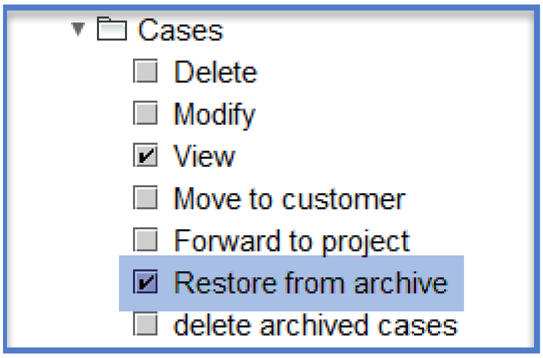
Archived Mails can be restored only by Agents who are authorized to do so and by the Administrators.

NOTE: Mails restored will get archived again, when the archive service runs in the background according to the setting done under the Archive tab.

2.3.1 Archive restoration by Agents

The right to restore archived mails needs to be assigned to an Agent. It can be assigned as follows:

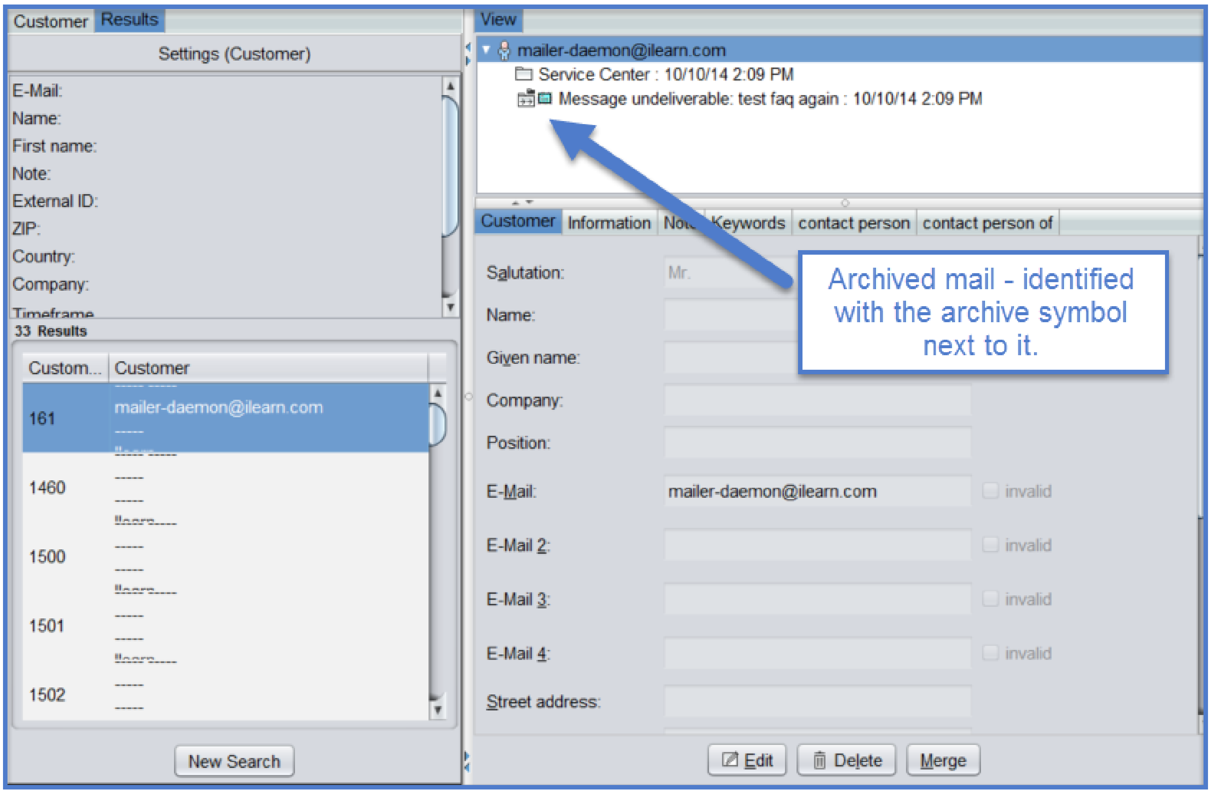
Administration → Agent → Edit → Rights → ServiceCenter → Projects → Select relevant project name → Cases → Restore from Archive



The archived mails can only then be restored by an authorized Agent by simply clicking on the archived mail. Please have a look at the screenshot below to understand the same.

Screenshot 1 – Archived mail seen in the customer search window.

Search → Customer → Show

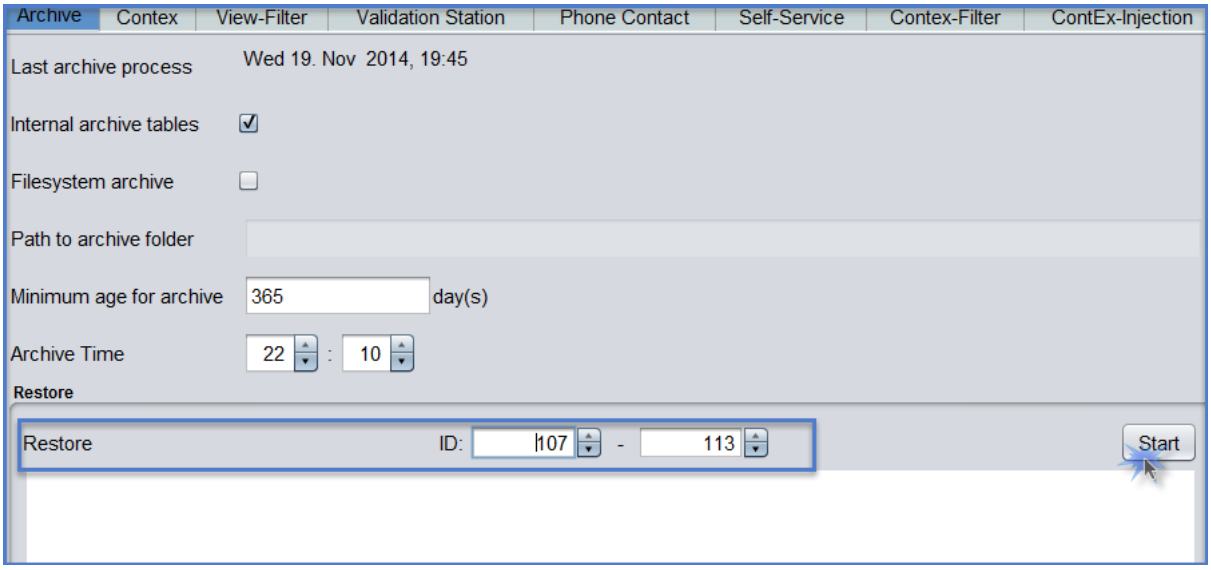


When an agent authorized to retrieve archived mails, clicks on this mail, the mail is restored and is displayed with the following symbol: 

It can now be processed. During the next archiving cycle, it will be archived again!

2.3.2 Archive restoration by Admin

Archived mails can be restored by the Admins by using the Archive tab.



Here they would find an option to enter ID of mails they want to restore.

Simply entering these IDs or range of IDs and then clicking on **START** will restore the mails archived with these IDs.

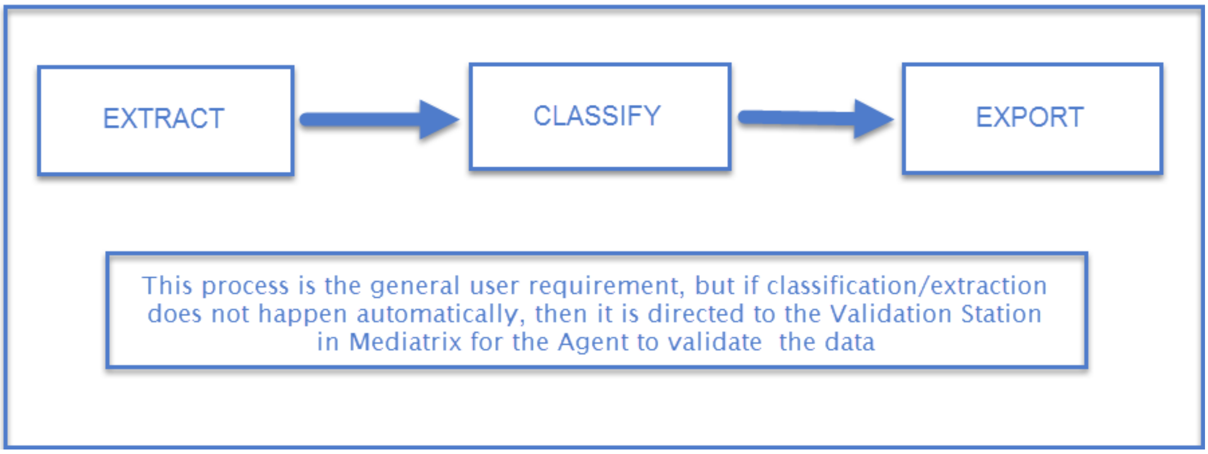
An Administrator can also retrieve mails by simply double clicking on the archived mails. This will restore the mails back to the mailbox.

3 Improved Default Validation Station (Mediatrix)

Mediatrix Validation Station is an extension in Mediatrix like Customer Portal or Team Management. It is available for the customers who are licenced to use the same.

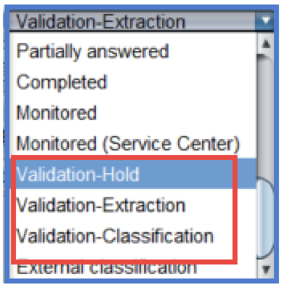
Validation Station can be used for Document Classification or Information Extraction.

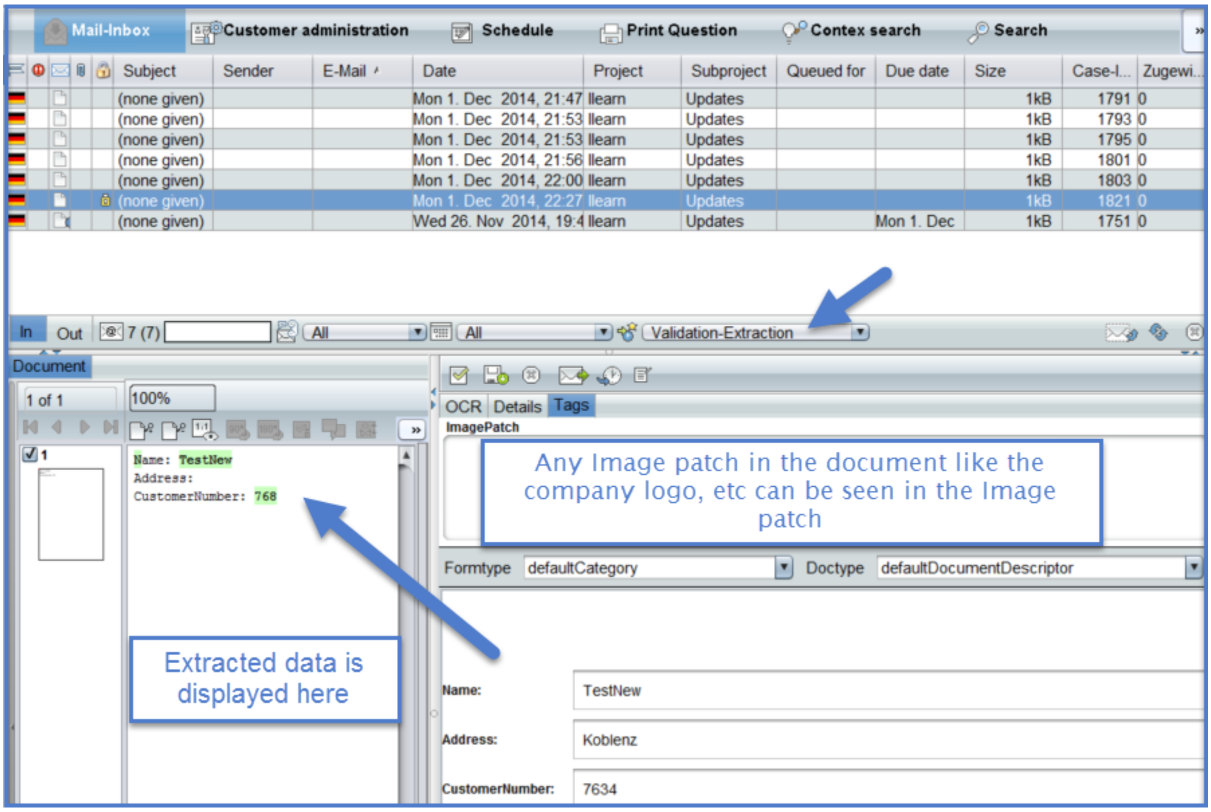
The documents to be classified or the documents from where the information is to be extracted are initially passed through an automated designed process using Contex, where the process defines conditions to sort the documents or extract information.



This process is the general user requirement, but if classification/ extraction does not happen automatically, then it is directed to the validation station in Mediatrix for the agent to validate the data. This is where Validation Station comes into picture. Validation Station is added as an extension to Mediatrix and has a user interface and administration interface.

User Interface is where the incoming documents for information extraction or classification are seen in the Mediatrix Inbox. The user has to choose the relevant option in the drop down filter to see the documents in the inbox. Please see the screenshot below.

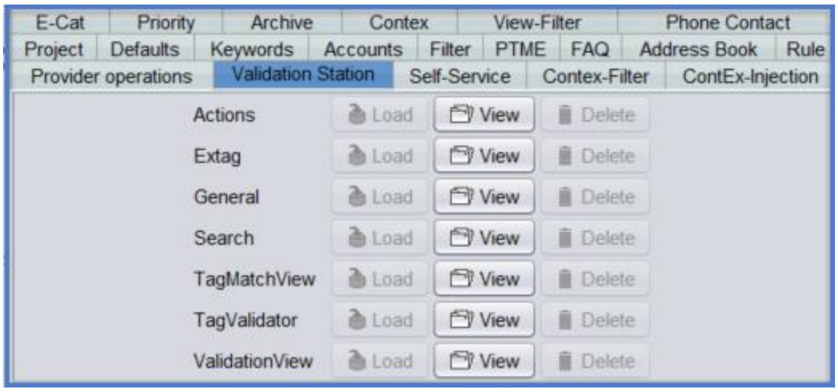




The user can access these documents and process the same manually. These documents are visible using the filters defined for the same.

3.1 Administration Interface

This interface is present for the validation station administration. Mediatrix Administrator can have rights to the same, but generally this tab is configured by the application developers for all customers.

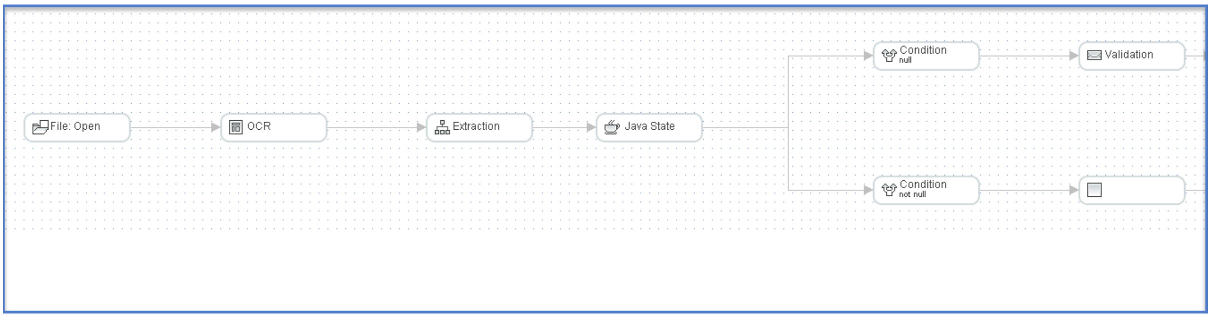


Every tab has a different functionality and is used to customize the look and feel of the Validation Station as per the customer requirement.

3.2 Designer Process

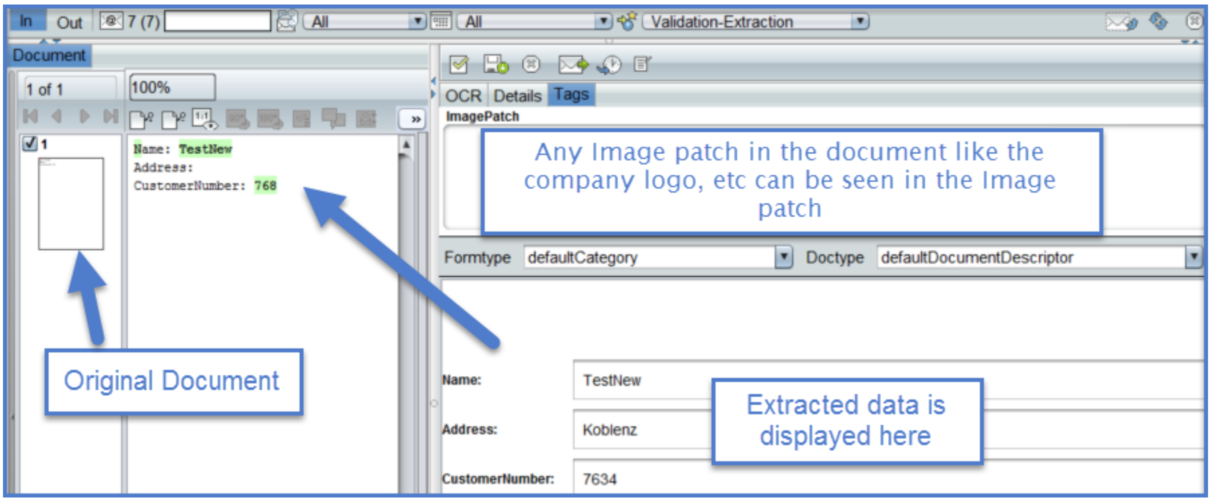
Designer process is a logical flow of nodes defined in the Contex designer, which lead to a desired end result. To know more about creating a designer process, please refer to the Context Manual.

In the screenshot below, we can see a Contex process defined for Validation Extraction.



Each node in the diagram below has a specific part of the task assigned, which has to be completed before the task can be forwarded to the next node. Finally the documents land in the Mediatrix Mailbox and are worked upon manually before they are further routed back to Contex.

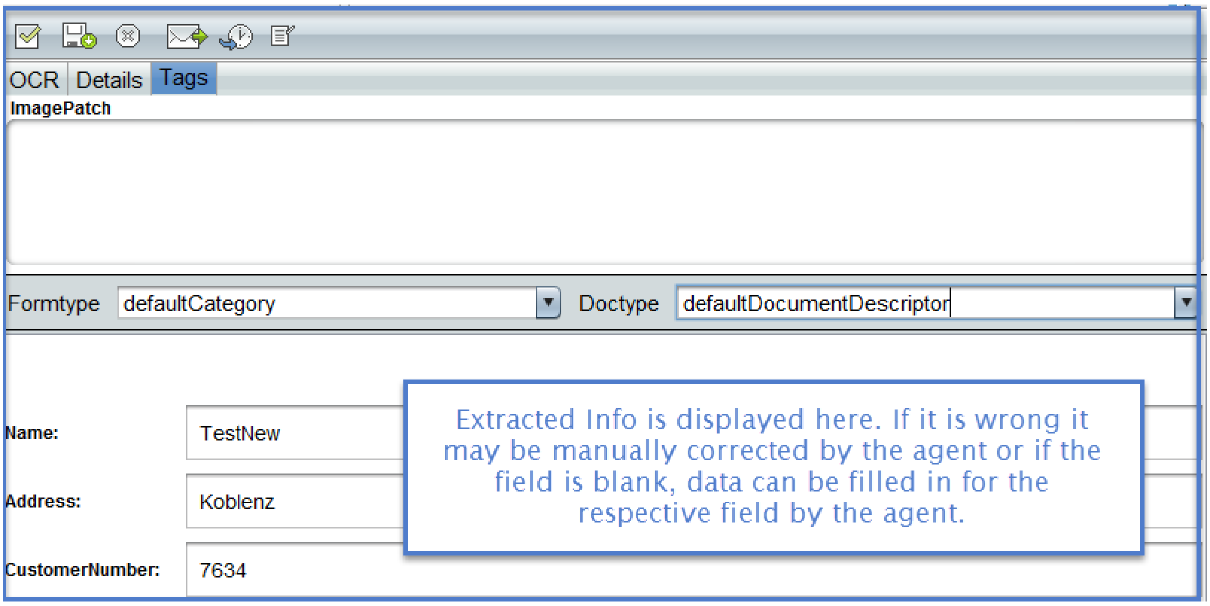
3.3 Validation Station – User Interface



3.4 Tags

The TagMatches defined under **Validation Administration –Tag Match View** (please refer to the Chapter 3.11) are displayed here with the matched information populated.

The user may change the populated information, if it is wrong or the user may enter the exact information, in cases where no data is populated at all.



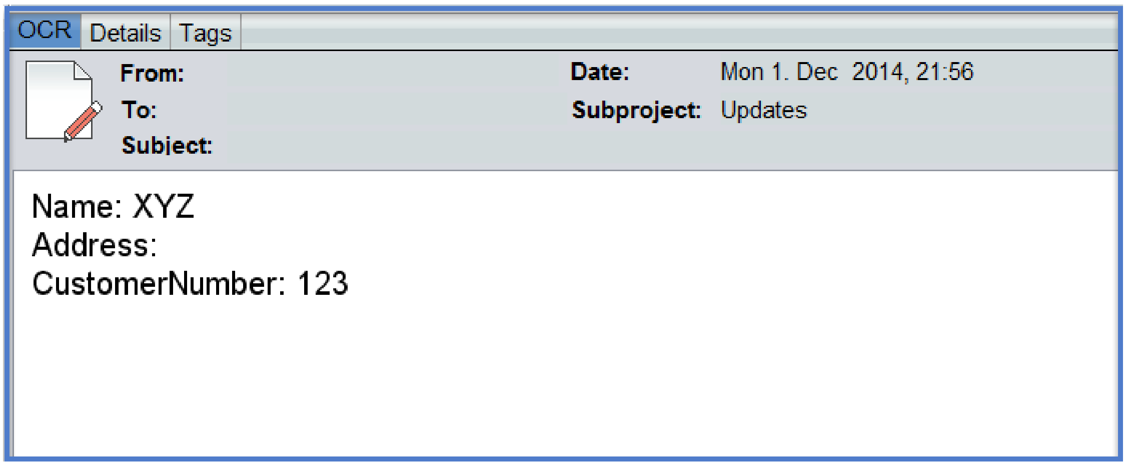
After doing the needful, the user can either

- COMPLETE: ,
- SAVE: ,
- CANCEL: ,
- FORWARD: ,
- REQUEUE: ,
- or CONFIGURE: 

the document accordingly.

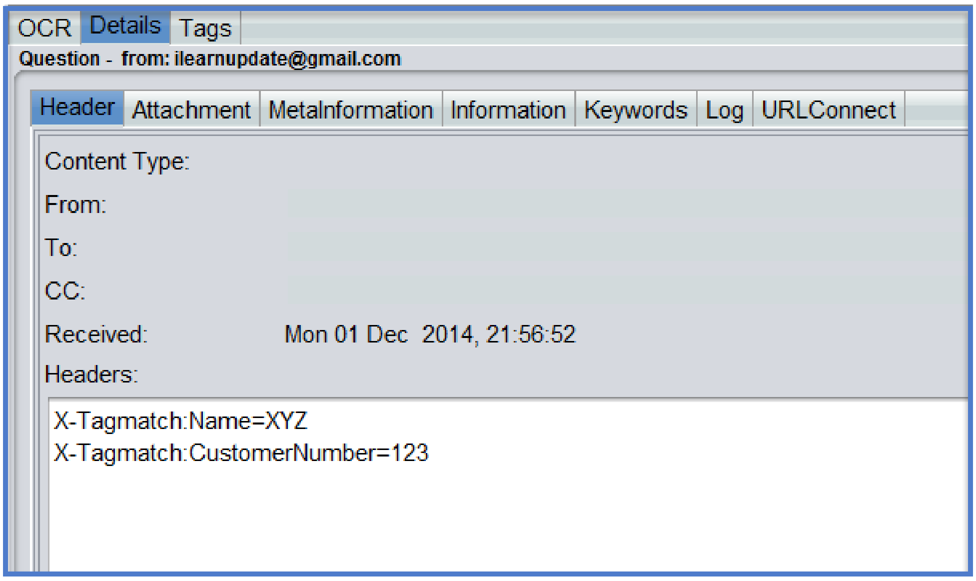
3.5 OCR

OCR displays he data extracted after OCR has been performed on the document.



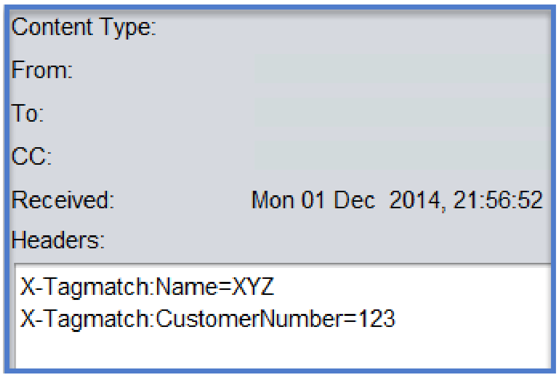
3.6 Details

The Details tab displays the Incoming Email details. Each of these tabs are explained in detail in the Operator and Mailbox Manual.



3.7 Header

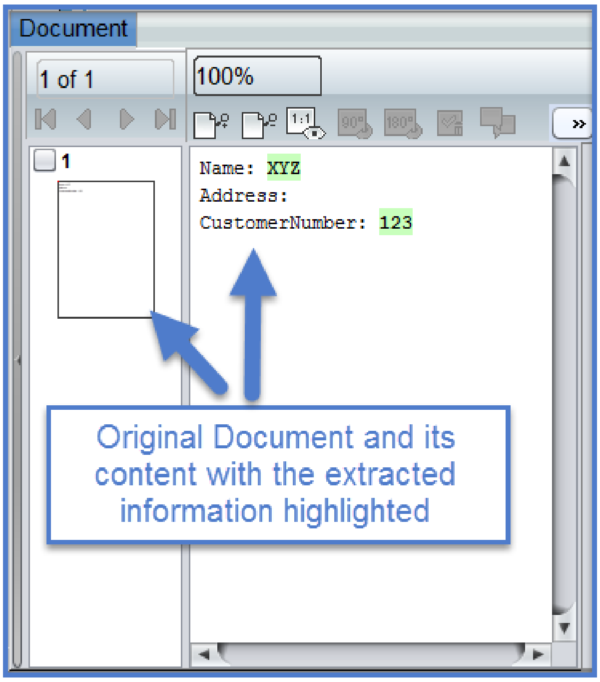
This tab displays the TagMatches defined and their respective values from the document.

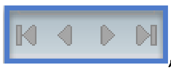


The screenshot above displays the TagMatch – Name and CustomerNumber with their respective values identified from the document.

3.8 Document

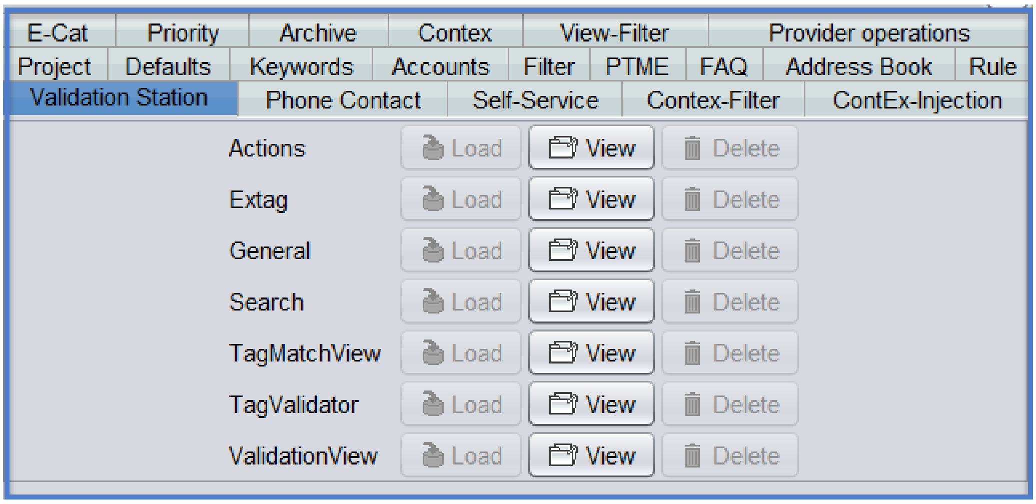
The incoming Document and the extracted Information are displayed in the user interface.



The document pages can be scrolled through using the arrow keys , correspondingly the display of the Information will change. This Information display can be zoomed, unzoomed, can be fitted to exact size or rotated using the following buttons - . Access to these buttons, depends on the agent authorization.

3.9 Validation Station – Administrative Interface

Administration → Project → Edit → Select a Project → Validation Station



The actual view of the data extraction and classification seen when the documents come into the Mediatrix mailbox is defined here.

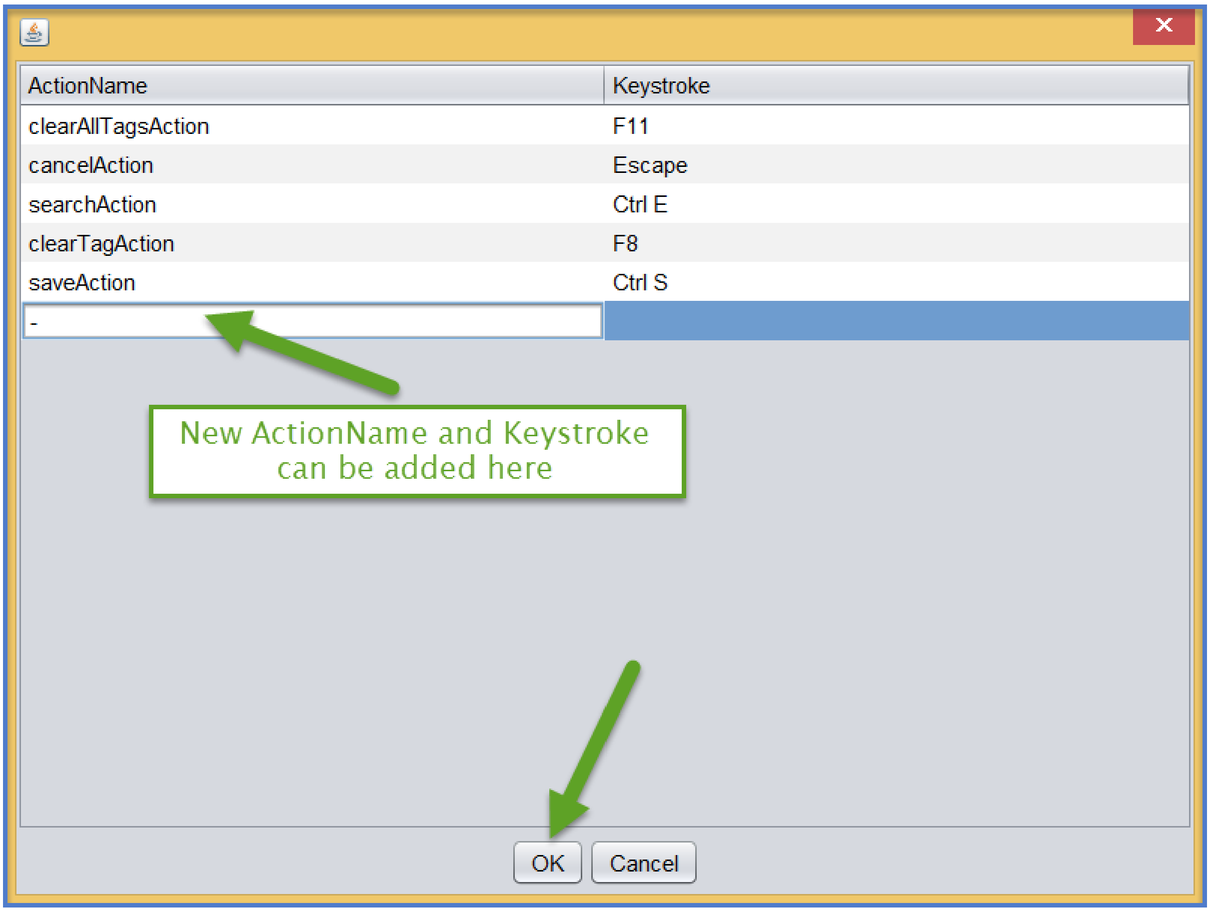
Each of these tabs have unique functionalities. The settings here are generally done by the Application Developers. Else, an Agent with Administration rights can access the same.

3.10 Actions

The action shortcut keys can be defined here. This enables using the specified keys to execute that specific action.

Customer also has the option to create a Notepad file specifying the shortcuts and actions thereof on his desktop. He can then **LOAD** this file using the load tab under Actions. Else he can **EDIT** the existing shortcuts.

If a customer clicks on the EDIT button, the following screen pops up. Here, one can see pre-defined shortcuts. They can be edited as per the customer requirement.

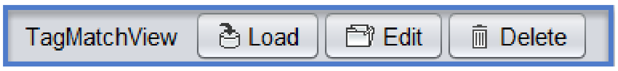


The shortcuts seen in the screenshot above are as follows:

- clearAllTagsAction = F11
- CancelAction = Escape
- SearchAction = Ctrl + E
- Clear TagAction = F8
- saveAction = Ctrl + S

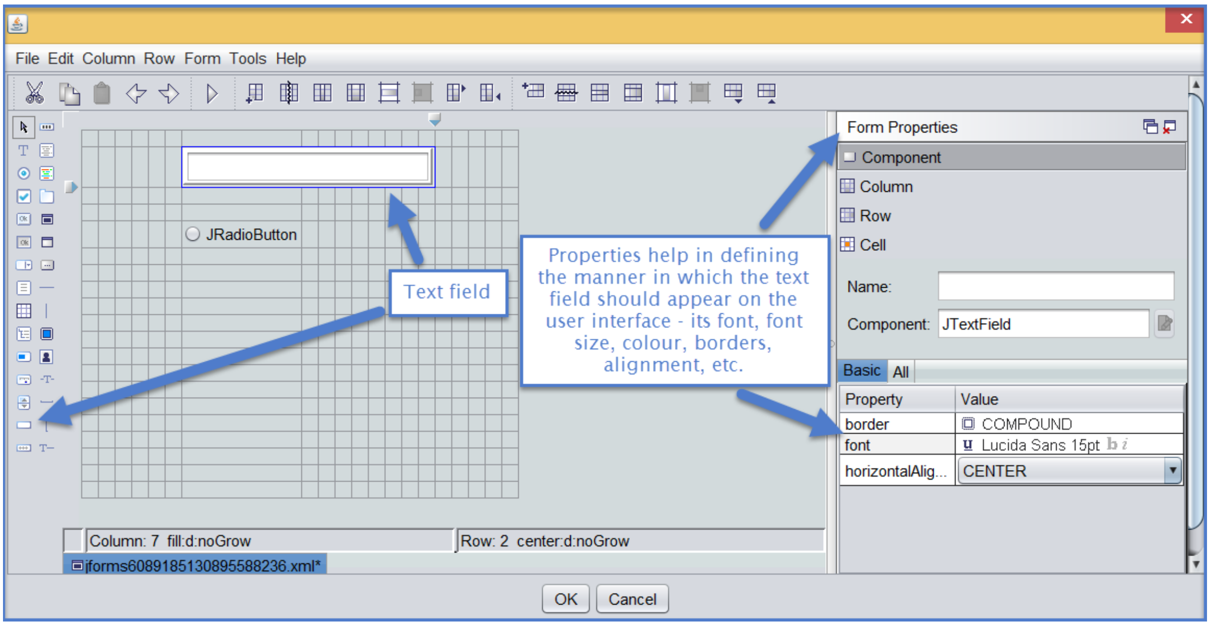
Customer can define shortcuts specific to his use too under Actions.

3.11 TagMatch View



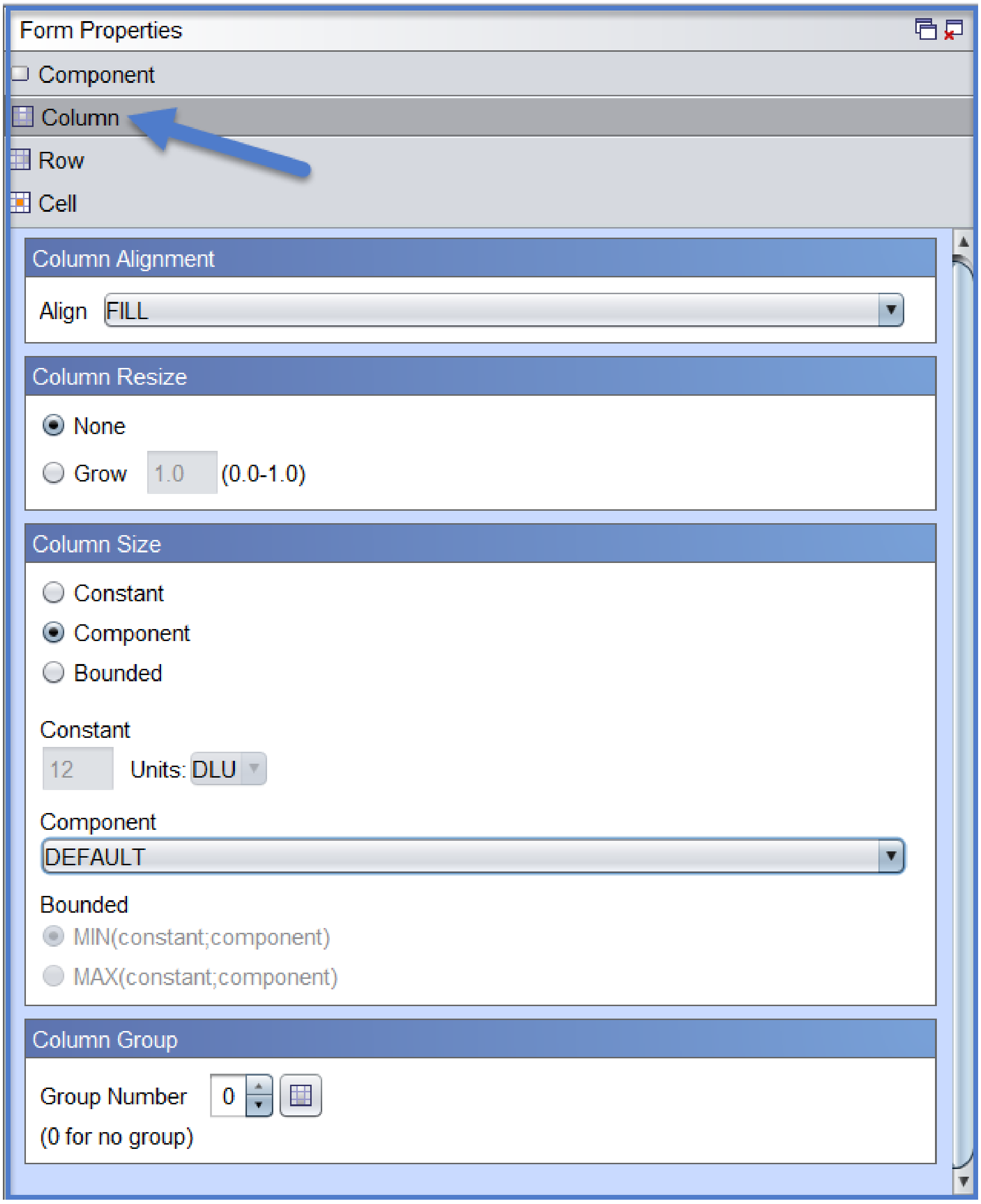
Tags visible on the user interface to display extracted Information are defined under TagMatch View.

Clicking on the **EDIT** tab, opens the **Abeille Designer**, which is used to define the look and feel of the user interface for **Information Extraction**.

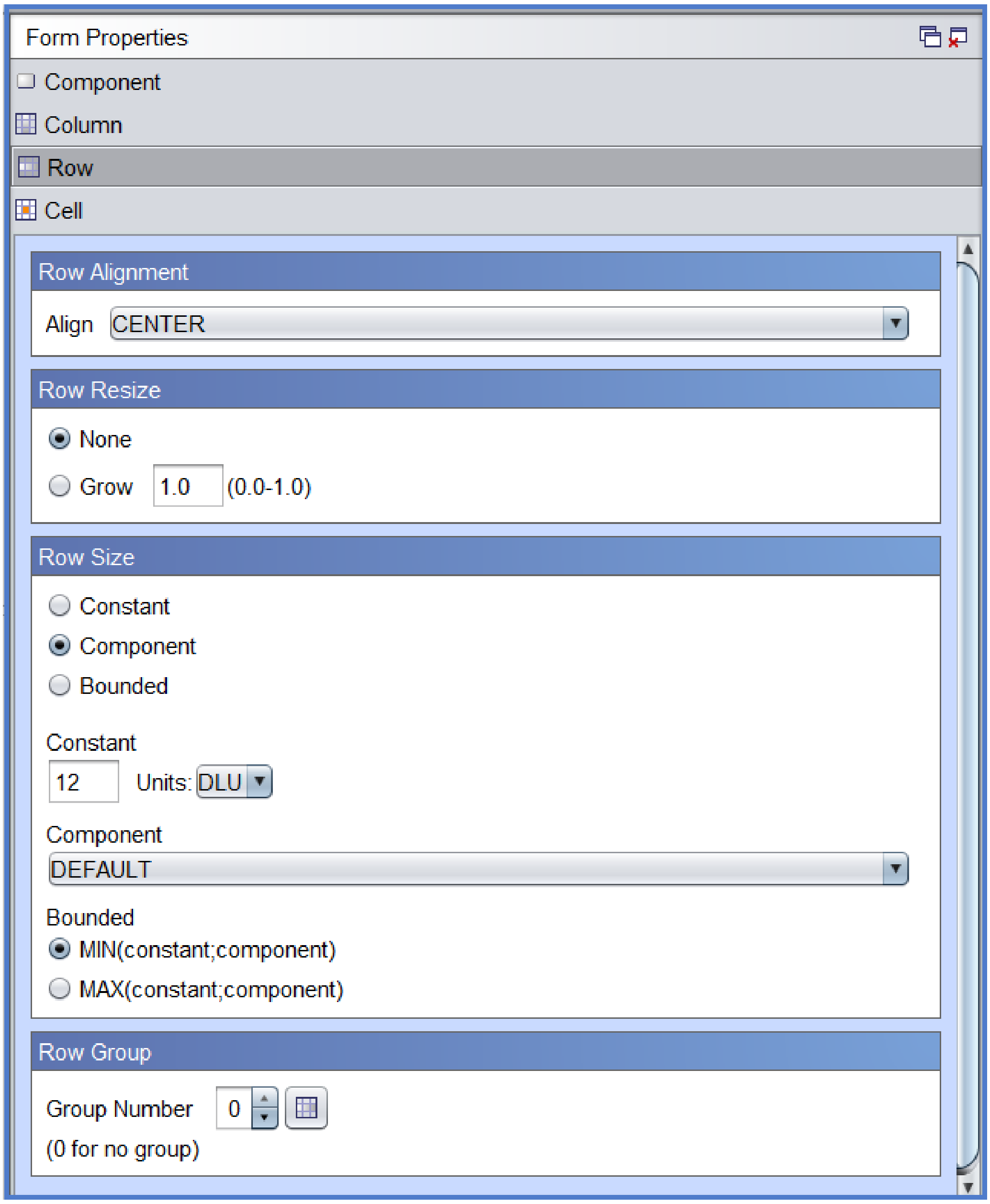


This Designer is used to define the tags – like text fields, radio buttons, combo boxes, image insertions, etc. as per the customer requirement. Each of these tags can be modified using the **FORM Properties** seen on the right hand side. Here one can define the size of the tag using the **Column** and **Row** option. The **Component** tab helps in defining the look of the Tag. Please find the respective screenshots below.

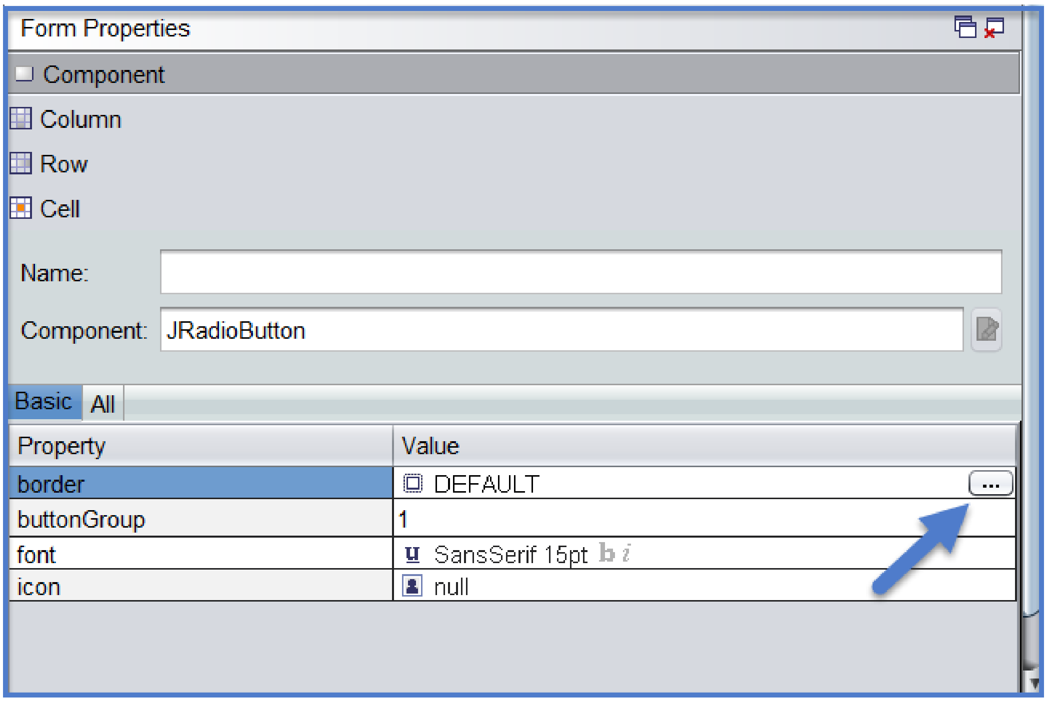
Column:


Form Properties
Component
Column
Row
Cell
Column Alignment
Align
FILL
Column Resize
None
Grow
1.0
(0.0-1.0)
Column Size
Constant
Component
Bounded
Constant
12
Units:
DLU
Component
DEFAULT
Bounded
MIN(constant;component)
MAX(constant;component)
Column Group
Group Number
0
(0 for no group)

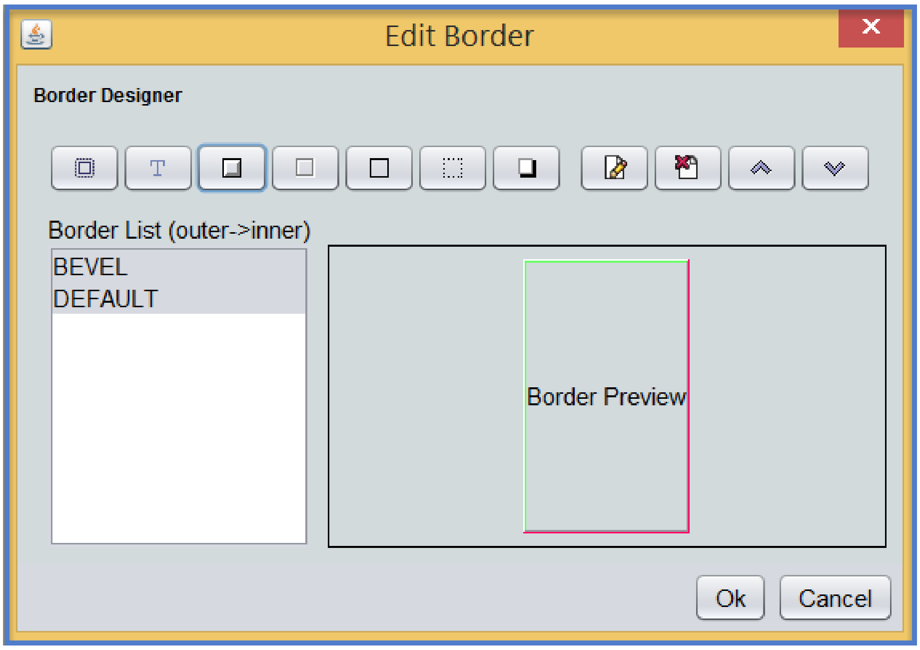
Row:


Form Properties
Component
Column
Row
Cell
Row Alignment
Align
CENTER
Row Resize
None
Grow
1.0
(0.0-1.0)
Row Size
Constant
Component
Bounded
Constant
12
Units:
DLU
Component
DEFAULT
Bounded
MIN(constant;component)
MAX(constant;component)
Row Group
Group Number
0
(0 for no group)

Component:



On clicking on the border tab, a window with additional option to define the tag border pops-up. The preview of the same is also displayed on the right hand side.



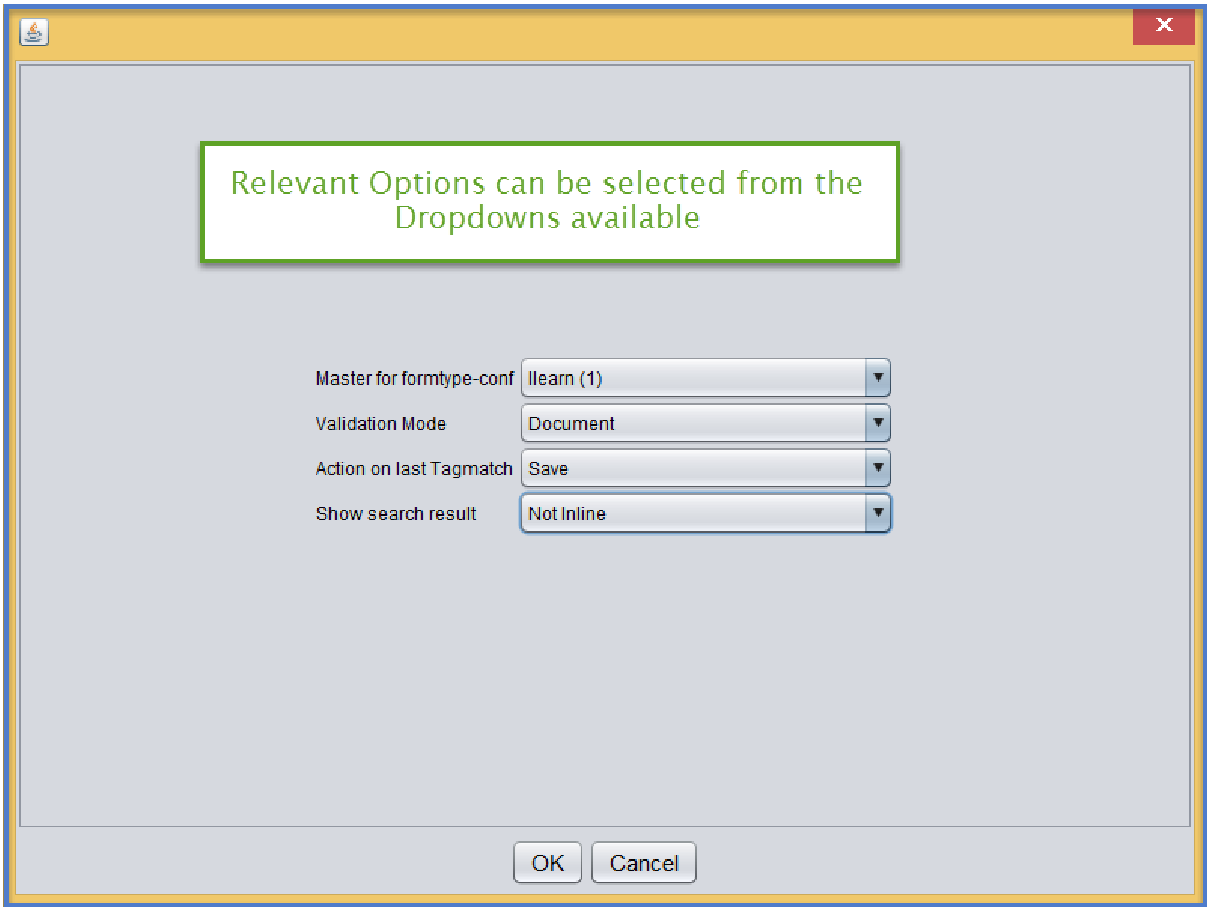
Similarly the **buttonGroup, Font** and **Icon** can also be defined.

A Customer can even design his own View using the Abeille Designer installed on his own machine. This same file can then be imported to Mediatrix – TagMatch View using the **LOAD** option.

3.12 General

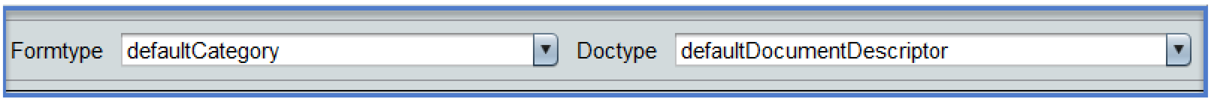
This tab is generally configured by the **Application Developers**.

On clicking the **EDIT** tab, the following Window opens. This Window has all the details mentioned, which are used for this customer. A new **NOTEPAD** file can also be imported to Mediatrix using the **LOAD** tab.



Master for formtype-conf:

This is where the Formtype and Doctype visible in the user interface as defined. Please refer to the screenshot in Chapter 3.4 for the same.



A default master is created in Contex for every project in Mediatrix. The Master chosen here in the General tab, refers to the Master of the Contex process defined for document classification or extraction in Contex. Correspondingly, we define the Master in the General tab.

Validation mode:

This mentions how a tag should be stored, once a document is saved or completed in Validation Station. The possible modes are – Document and Container. Generally Container is mentioned as Default mode.

Saving lasttagmatch:

This specifies if a document should be saved, when the user presses the Tab button on the last TagMatch. If lasttagmatch.save is set to FALSE, the option is disabled. If it is set to TRUE, then this option is enabled for the user.

Fuzzy search result display:

A User may want the result of the Fuzzy Matcher to be displayed in a separate window as Pop-Up or in the same window. This setting is saved here. This also depends on the number of records to be displayed. Thus, when searchresult.inline is set to TRUE, the results are displayed in the same window, else in a separate pop-up window.

3.13 Search

The configuration of this tab too, is generally done by the Application Developers. Depending on the customer requirement, a search method is defined – fuzzy or some other.

After the records are searched for and the customer clicks on them, they get saved to records automatically.

Master and Namespace configuration:

A default master is created in Contex for every project in Mediatrix. The Master chosen refers to the Master of the Contex process defined for document classification or extraction in Contex. Namespace may be defined as the group of labels which need to be extracted or searched for from the database.

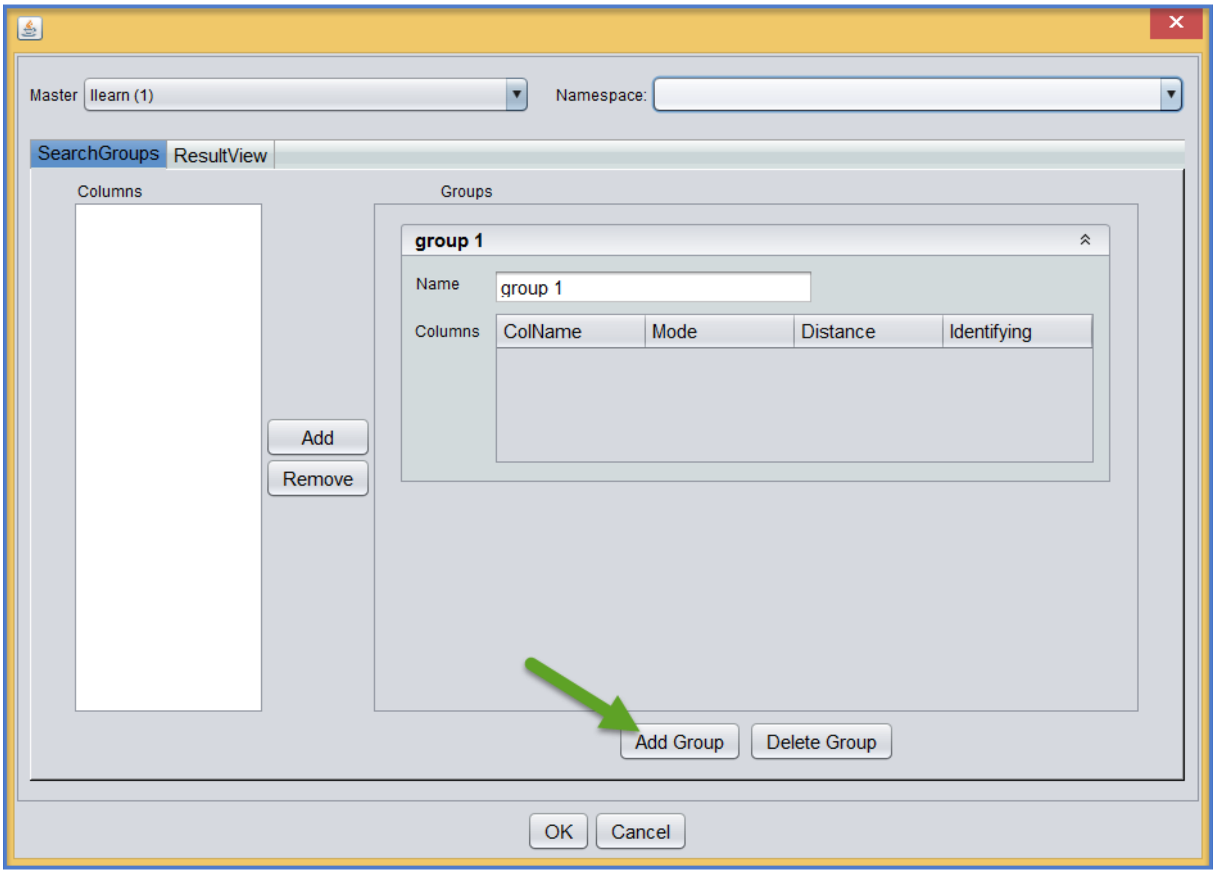
Namespace = cities, denotes that the search is going to be for the label cities. We can specify the label to be searched for as per our requirement.

Columns:

Under this section, how the columns should be looked in the FuzzyMatcherService.

The format entered for the same is as follows:

MODE, DISTANCE, IDENTIFYING



Mode is the means by which the search will be initiated. Options available are **FUZZY: 0, REGEX: 1, PREFIX: 2** and **EXACT: 3**.

Distance can be any numerical like 0, 1, 2, etc. Distance specifies the maximum distance between given column value and indexed value. In simple words, it is the number of characters that can be ignored for displaying results during search.

Identifying is used to display the search result. If Identifying is **TRUE** – then the search results with the mentioned distance will be displayed, if it is FALSE – then the search with the mentioned distance will be ignored, only the exact search, if found will be displayed.

For e.g. City = 0, 1, true [Namespace = mode, distance, identifying]

If we want the fuzzy matcher to search in the Column CITY, for the name ANI, with a distance of 1, where identifying is TRUE - then the possible results getting displayed after search are – **ANI**, AN**U**, **M**NI and A**L**I.

4 Single Sign On (Mediatrix)

SSO vanished from Mediatrix v2.2 because of security reasons, in v2.4 it will be reintroduced to Mediatrix.

Following login methods are supported

- Native mediatrix accounts
- Windows Authentication
- Authentication based on Kerberos tokens

The prefered method may be chosen at client login, the default method can be defined by setting the mediatrix.properties key “authentication.methods”.

4.1 Tutorial

- Create a service user for ITyX services like „ITyX WebApp“ (in this example the user will be called „serviceuser“). In the configuration choose “password never expires”, in order to make maintenance easiser
- Create a service principle: `setspn -a service/server.domain.local@DOMAIN.LOCAL serviceuser`
- Create a keytab for your newly created user with login credentials: `ktpass -princ service/server.domain.local@DOMAIN.LOCAL -pass PASSW0RD -mapuser serviceuser@DOMAIN.LOCAL -out c:\keytab -ptype KRB5_NT_PRINCIPAL -crypto RC4-HMAC-NT`
- To check the service principal: `setspn -L serviceuser`
- Copy the created keytab to the computer, which hosts the Mediatrix Service (WebApp). It will be needed, so that the service can log onto the KRB5 server

The computer needs to receive adjustments to the registry, that TGT will be stored for future use.

http://www.javaactivedirectory.com/?page_id=93

4.1.1 Windows XP

To the Kerberos key, add a new DWORD_VALUE called "allowtgtsessionkey", and assign it a value of 1.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\
REG_DWORD name: allowtgtsessionkey
Value: 1
```

4.1.2 Windows 2000 and 2003 Server

To the Parameters key, add a new DWORD_VALUE called "allowtgtsessionkey", and assign it a value of 1.

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
REG_DWORD name: allowtgtsessionkey
Value: 1
```

4.2 mediatrix.properties

Possible mediatrix.properties values to configure Single Sign On are:

Property	Description	Values	Default
authentication.methods	Defines which authentication methods are supported. They will appear in the Mediatrix Client login screen. If multiple methods are to be allowed, they can be chained with comma. e.g. WINDOWS,MEDIATRIX	WINDOWS, KERBEROS, MEDIATRIX separated by comma	MEDIATRIX
authentication.realm	Authentication Domain	Any string in uppercase	
authentication.keydistribution	Name of the key distribution server	Any string in lowercase	
authentication.clientconfdir	Path to krb5.conf	Any valid path to a file	/etc/krb5.conf
authentication.keytabfile	Path to keytab file	Any valid path to a file	/etc/keytab
authentication.serviceprincipal	principal name that was used for Mediatrix	Any string	mxservice

5 Security Layer (Contex)

In v2.4 Contex provides a secure Login-System for “Contex Admin”. Access to the program does no longer provide every option to change configuration. Access to each Contex module may be restricted.

5.1 Authorization / Roles

Access to Contex modules is organized within roles. Each role has the same name like the Contex module it provides. If a user has e.g. the role “ICAT”, he is allowed to reconfigure / use the Categorizer module. If the ICAT role is not provided, the user cannot change anything within the Categorizer configuration.

Following roles are available:

- **ADMIN** – A special role, it contains full access to the system
- ADMINISTRATION
- MONITORING
- DOCUMENT
- SCHEDULER
- DESIGNER
- ICAT
- MCAT
- VCAT
- IFORM
- EXTAG
- ITAG
- FUZZY
- OCR
- VOCR
- CLUSTERING
- IDIG
- NORMALIZER

If a role is not provided for a certain user, the Contex module will be made inaccessible (invisible).

5.2 Authentication

Following authentication methods are available

- Internal – the Contex authentication, using Contex accounts
- Windows – User/Password authentication via Windows domain controller, roles are provided via group policies
- Kerberos – User/Password authentication via Windows domain controller / Kerberos, Roles are provided via LDAP, SingleSignOn is possible

The configuration of these authentication methods must be done on the Server that hosts the ITyX ManagementServer (License Service)

There is a new directory containing several configuration files

`mediatrix-contex/conf/login-service`

4 files within:

- `login-service.properties`
- `rolemapping.xml`
- `internal-users.xml`
- `kerberos-authentication-configuration.xml`

All authentication methods available for users have to be declared in the file „login-service.properties“. The prefered method(s) must be set set on true:

```
#################### Internal authentication ####################
#
# To configure users, passwords and roles see 'internal-users.xml'
#

# set to 'true' to enable Internal authentication
internal.enabled=true

    .
    .
    .

#################### Kerberos authentication ####################
#
# to configure the mapping from LDAP group to contex role see
'rolemapping.xml'
#

# set to 'true' to enable Kerberos authentication
#kerberos.enabled=true

    .
    .
    .

#################### Windows authentication ####################
#
# to configure the mapping from Windows group to contex role see
'rolemapping.xml'
```

```
#

# set to 'true' to enable Windows authentication
#windows.enabled=true
```

5.2.1 Internal

If this method is enabled, users, passwords and roles will be drawn from the file `internal-users.xml`. New users must be inserted using a proper xml syntax (example below).

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:context="http://www.springframework.org/schema/context"
    xmlns:security="http://www.springframework.org/schema/security"
    xmlns:util="http://www.springframework.org/schema/util"
        xsi:schemaLocation="http://www.springframework.org/schema/security
http://www.springframework.org/schema/security/spring-security-3.2.xsd
                                http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-4.1.xsd
                                http://www.springframework.org/schema/util
http://www.springframework.org/schema/util/spring-util-4.1.xsd
                                http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context-4.1.xsd">

     <!-- Here you can define users and roles/authorities for 'Internal'
authentication.                    -->

     <!-- Available authorities:      ADMINISTRATION, MONITORING, DOCUMENT,
SCHEDULER, DESIGNER, ICAT,      -->
    <!--                               MCAT, VCAT, IFORM, EXTAG, ITAG, FUZZY,
OCR, VOCR, CLUSTERING,          -->
        <!--                                                           IDIG,
NORMALIZER                                                    -->
    <security:user-service id="internalUserService">
        <security:user
            disabled="false"
            name="admin"
            password="ityx"
            authorities="ADMIN"
        />
        <security:user
            disabled="true"
            name="user"
            password="ityx"
             authorities="ADMINISTRATION,MONITORING,DOCUMENT,SCHEDULER,DESIG
NER,ICAT,MCAT,VCAT,IFORM,EXTAG,ITAG,FUZZY,OCR,VOCR,CLUSTERING,IDIG,NORMALIZ
ER"
```

```
        />
    </security:user-service>

</beans>
```

Example: If you need another user to access “Contex Scheduler”, but no other module, add following contents to the xml tag <security:user-service>

```
        <security:user
            disabled="true"
            name="user"
            password="ityx"
           authorities=" SCHEDULER"
        />
```

5.2.2 Windows

Users can be authenticated via Windows domain controllers. Each role will be issued by a group from the domain itself. It is possible to issue multiple roles to one group.

In order to map the domain groups to a role set of Contex, configuration in the file `rolemapping.xml` is required.

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:util="http://www.springframework.org/schema/util"
            xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans-4.1.xsd
                                  http://www.springframework.org/schema/util
http://www.springframework.org/schema/util/spring-util-4.1.xsd">


     <!-- Here you can define the 'Contex' roles/authorities which will be
granted                  -->
              <!--    for   the    membership    in    a    LDAP    /    Windows
group.                                                   -->

          <!--   These   roles   are   used   only   by   Windows   and   Kerberos
authentication.                         -->

   <!-- Available roles:    ADMINISTRATION, MONITORING, DOCUMENT, SCHEDULER,
DESIGNER, ICAT,      -->
    <!--                        MCAT, VCAT, IFORM, EXTAG, ITAG, FUZZY, OCR,
VOCR, CLUSTERING,          -->
          <!--                                                          IDIG,
NORMALIZER                                                            -->
    <util:map id="roleMap" value-type="java.lang.String[]">
        <entry key="ITYX\Contex" value="ADMIN" />
```

```
        <!--
        <entry key="ITYX\Mediatrix" value="ICAT, VCAT" />
        -->
    </util:map>

</beans>
```

5.2.3 Kerberos

Kerberos authentication makes use of AD/Kerberos users. Role allocation is configured via the `UserDetailsService`. The designated user groups are mapped to Contex roles – the same mapping takes place in Windows authentication (chapter 5.2.2).

In order to use Kerberos authentication several parameters must be set in the file `login-service.properties`. Important properties are:

- `KDC`
- `REALM`
- `Servicename`

You also need to configure credentials and search filters for your LDAP server. To check the authenticity of the Kerberos Service Ticket you also need to declare a valid path to the `keytab` file.

```
    .
    .
    .

#################### Kerberos authentication ####################
#
# to configure the mapping from LDAP group to contex role see
'rolemapping.xml'
#

# set to 'true' to enable Kerberos authentication
#kerberos.enabled=true

# path to keytab location of kerberos service user
('file:/PATH/TO/KEYTABFILE')
#kerberos.keytab.location=file:/PATH/TO/KEYTABFILE

# hostname of key distribution center (FQHN!)
#kerberos.kdc=kdc.example.com

# kerberos relam name (caseSensitive!)
#kerberos.realm=EXAMPLE.COM
```

```
# kerberos service name
#kerberos.servicename=cxservice

# enable ticket cache on client (SSO)
#kerberos.useticketcache=true

# default role that will be granted if no UserDetailsService is provided (see
'kerberos-authentication-configuration.xml')
#kerberos.defaultrole=ADMIN

# URL of LDAP including root DN
#kerberos.ldap.url=ldap://example.com:389/CN=Users,DC=EXAMPLE,DC=com

# distinguished name (DN) of ldap manager account
#kerberos.ldap.manager.dn=cn=Administrator,cn=Users,dc=EXAMPLE,dc=com

# password of ldap manager
#kerberos.ldap.manager.password=Ityx1234

# search filter used to find user (defaults to '(CN={0})', parameter will be
substituted with current users name)
#kerberos.ldap.user.filter=(CN={0})

# search base for user filter (defaults to '')
#kerberos.ldap.user.base=

# group filter used to determine the group memberships of current user.
Parameter will be substituted with users DN. (defaults to '(member={0})')
#kerberos.ldap.group.filter=(member={0})

# search base for group membership searches
#kerberos.ldap.group.base=

    .
    .
    .
```

Realm is caseSensitive.

5.2.4 SingleSignOn

Using the property `useTicketCache` it is possible to use SingleSignOn with Contex. Contex uses the Kerberos Ticket Cache if that property is set to `true`. If a Kerberos TGT is found, no login is necessary.

In Windows Contex usually looks for a file named `krb5cc_USERNAME` in ist Userhome directory, for example c:\Users\Ityx\kr5cc_Ityx. If the file cannot be found, Contex looks for credentials in the Windows LSA.

The ticket cache within the userhome directory can be created with the tool `kinit`, which comes with a Java SDK installation. The generated TGT must be 'proxiable' (-p) and 'forwardable' (-f).

Because of problems with the Windows UAC `useTicketCache` cannot be used as a local Windows Administrator in combination with Windows LSA. Only a ticket cache generated with `kinit` is usable.