

# IMPLEMENTING FORENSIC MODE

After making decision on the infrastructure for the forensic mode and inputs from legal and IT departments several mail boxes will need to be created. To better demonstrate the implementation process, we will use a made up organization Best Interpreters, Inc. with bestinterpreters.com domain.

## CREATE FORENSIC MAILBOXES

Using recommended infrastructure we will create 3 mailboxes:

- [forensic.staff@bestinterpreters.com](mailto:forensic.staff@bestinterpreters.com) - this mailbox will retain all internal communication initiated by ScheduleInterpreter®;
- [forensic.client@bestinterpreters.com](mailto:forensic.client@bestinterpreters.com) - this mailbox will retain all communication sent out by ScheduleInterpreter® to the requesters and administrative team of the account, division or business unit;
- [forensic.vendor@bestinterpreters.com](mailto:forensic.vendor@bestinterpreters.com) - this mailbox will retain all communication sent out by ScheduleInterpreter® to the vendors.

## ASSIGN RIGHTS TO ACCESS

IT department will need to assign access rights to share content of the mailboxes with people who should be able to retrieve messages from the forensic mailboxes.

## DEFINE RETENTION POLICIES

This process may require participation of representative of your compliance, legal and IT departments. When retention policy is defined, use your mail server to automate how long the messages in the forensic boxes should be stored. A screenshot below demonstrates configuration of the policies using Microsoft Office 365.

The screenshot shows the 'Options' menu on the left with 'Mail' expanded and 'Retention policies' selected. The main area is titled 'Retention policies' and contains a table of existing policies. Below the table, a detailed view for the '1 Month Delete' policy is shown, indicating it was assigned by an administrator and cannot be removed. The policy details specify that after the message is received, it is kept for 30 days, and after the retention period, it is deleted (temporarily recoverable).

Name	Retention action	Retention period
1 Month Delete	Delete	30 days
1 Week Delete	Delete	7 days
1 Year Delete	Delete	1 year
5 Year Delete	Delete	5 years
6 Month Delete	Delete	6 months
Never Delete	Delete	Unlimited

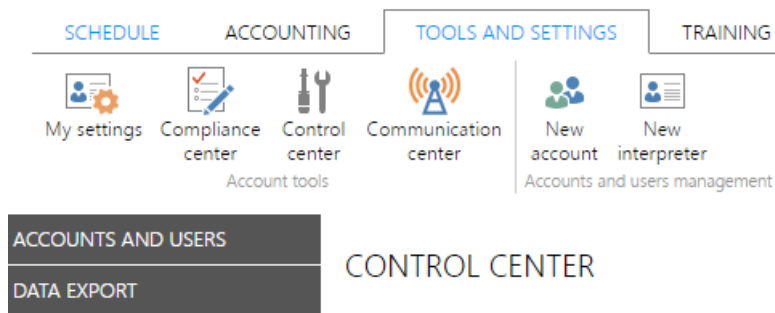
**1 Month Delete**  
This policy was assigned by your administrator and can't be removed.

**After the message is received:**  
30 days



**After the retention period:**  
Delete (temporarily recoverable)

## ADDING FORENSIC MAILBOXES TO YOUR ACCOUNT

Navigate to TOOLS AND SETTINGS > Control center > ACCOUNT SETTINGS > STAFF MEMBERS.



Click on ADD NEW STAFF button and complete the form. The image below demonstrates completed form of forensic mailbox for communication initiated by ScheduleInterpreter® for your organization staff members.

	TITLE	<input type="text"/>	<input data-bbox="502 660 539 698" type="button" value="?"/>
*	FIRST NAME	<input type="text" value="Forensic"/>	<input data-bbox="742 728 778 766" type="button" value="?"/>
*	LAST NAME	<input type="text" value="Staff"/>	<input data-bbox="742 801 778 840" type="button" value="?"/>
*	USER NAME	<input type="text" value="forensic.staff"/>	<input data-bbox="742 875 778 913" type="button" value="?"/>
*	USER TYPE	<input type="text" value="Super Administrator"/>	<input data-bbox="654 949 691 987" type="button" value="?"/>
	REVIEW TIER LEVEL	<input type="text" value="Tier 1"/>	<input data-bbox="518 1023 555 1061" type="button" value="?"/>
*	E-MAIL	<input type="text" value="forensic.staff@bestinterpreters.com"/>	<input data-bbox="742 1095 778 1133" type="button" value="?"/>
*	BRANCH	<input type="text" value="Main office"/>	<input data-bbox="630 1169 667 1207" type="button" value="?"/>
*	PHONE	<input type="text" value="7074000503"/>	<input data-bbox="638 1243 675 1281" type="button" value="?"/>
	SERVICES TO MANAGE	<input checked="" type="checkbox"/> Face-to-face <input checked="" type="checkbox"/> OPI <input checked="" type="checkbox"/> VRI	<input data-bbox="790 1310 826 1348" type="button" value="?"/>
	VENDOR PROFILE	<input type="checkbox"/>	<input data-bbox="454 1382 491 1420" type="button" value="?"/>
	ACTIVE	<input checked="" type="checkbox"/>	<input data-bbox="454 1449 491 1487" type="button" value="?"/>
	BLOCKED	<input type="checkbox"/>	<input data-bbox="454 1516 491 1554" type="button" value="?"/>
	DELETED	<input type="checkbox"/>	<input data-bbox="454 1583 491 1621" type="button" value="?"/>
	RECEIVE E-MAILS	<input checked="" type="checkbox"/>	<input data-bbox="454 1650 491 1688" type="button" value="?"/>
<input checked="" data-bbox="124 1736 571 1769" type="button" value="SHOW COMMUNICATION SETTINGS"/>			
*	PASSWORD	<input type="password" value="....."/>	<input data-bbox="638 1803 675 1841" type="button" value="?"/>

Complete setting other forensic mailboxes you have created.



To activate notification you have to login into ScheduleInterpreter® using each forensic mailbox account. This is a requirement per FCC regulation.

## DEFINE AND CREATE MESSAGE TAGS

Tag is a combination of letters, numbers or both included as text into the body of the message.

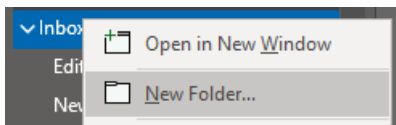
The process of creating robust filtering system will require planning of how the messages are going to be tagged. When implementing forensic mode, each message should include a unique tag. The simplest way is to include a tag into the body of the message. Most of the modern mail servers can read the content and filter the message if specific combination of letters, numbers or both is found. Including tag in the body of the message has another benefit, it is searchable using any modern e-mail client.

ScheduleInterpreter® recommends the format of tagging the messages that starts with two letters SI and includes two letters identifying the type of message and two letters identifying the recipient separated by the "-" dash symbol. For example, new request for staff members will have a tag SI-NR-ST, for requester or a client SI-NR-RQ and for a vendor SI-NR-VD. Similarly, cancellation notifications would be tagged SI-CL-ST, SI-CL-RQ and SI-CL-VD.

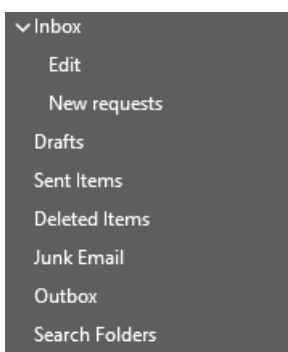
## BUILD FILTERS

Mail servers can vary dramatically in how they allow to filter and organize the messages. In this example, we use Microsoft Outlook to demonstrate the configuration settings. This configuration can be completed by the mail server administrator and may only require instructions on which forensic mailbox receives what message.

Use Microsoft Outlook to login to the forensic mailbox for staff members. Right click on the Inbox folder, select New Folder... option.



When place is created for a new folder enter New requests and hit Enter on your keyboard. Outlook will add the folder in a tree like structure, similar to the one shown below.




Add folders for each task from COMMUNICATION CENTER you would like to utilize forensic mode.

When all folders are added, use File menu to begin adding filters.



Locate and click on Rules and Alerts option

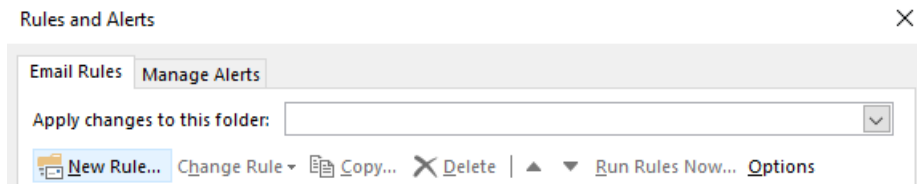


Manage Rules  
& Alerts

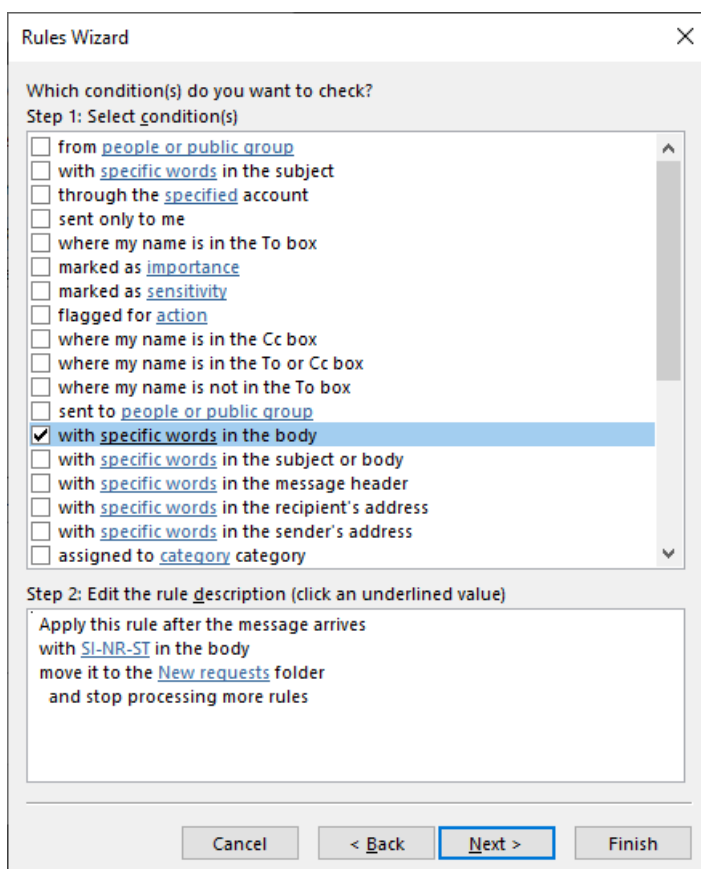
## Rules and Alerts

Use Rules and Alerts to help organize your incoming email messages, and receive updates when items are added, changed, or removed.

When Rules and Alerts window pops up, select your forensic mailbox from the Apply changes to this folder and click on New Rule... link.



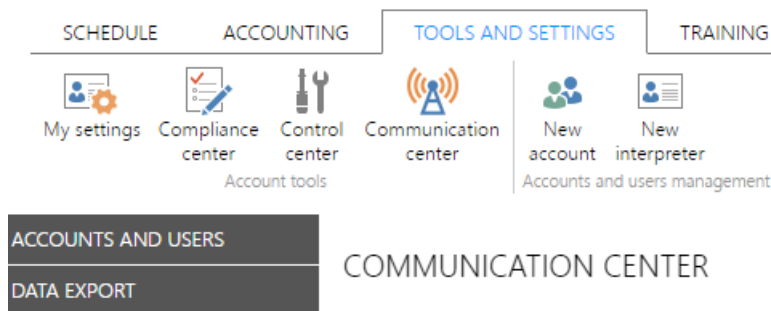
Complete configuration of the filter by selecting With specific words in the body and New requests in the folder. Your final selection should look like the one below.



Click Next > button to fine tune your filter or click Finish button to complete the settings. Use similar steps to complete filters for all other tags. Identical process is needed for clients, vendors and consumers.

## TAGGING MESSAGES

Login to your account in ScheduleInterpreter® with super administrator rights. Navigate to TOOLS AND SETTINGS > Communication center



Locate series of tabs listing communication events. These tabs have NEW, ASSIGN VENDOR, EDIT and other events as their names. Navigate to SCHEDULE > NEW > STAFF and locate REQUEST DETAILS field. It is a text field and you include any content in it.

\* REQUEST DETAILS

Dear {rcptSalutation},

{apptDigestTotal} new request(s) for services. Details are listed below.

{apptDigestContent}

{senderOrganization}

{senderFirstName} {senderLastName}

E-mail: {senderEmail}

Phone: {senderPhone}

On-line: {senderWebsite}

Scroll to the bottom of the REQUEST DETAILS field and starting from new line include the tag you selected or use the one recommended by ScheduleInterpreter®. After change, your message may look like this:

\* REQUEST DETAILS

Dear {rcptSalutation},

{apptDigestTotal} new request(s) for services. Details are listed below.

{apptDigestContent}

{senderOrganization}

{senderFirstName} {senderLastName}

E-mail: {senderEmail}

Phone: {senderPhone}

On-line: {senderWebsite}

SI-NR-ST

REQUEST DETAILS field is capable of accepting HTML content. You can minimize visibility of the tag by reducing the font size. Use following code to make the content of the tag smaller.

```
<span style="font-size:5px">NT-ST</span>
```

Make sure to click on SAVE CHANGES button to store your settings in ScheduleInterpreter®.

## ACTIVATING FORENSIC MODE

When configuration is completed, navigate to TOOLS AND SETTINGS > Communication center > SCHEDULE > NEW > STAFF and locate BCC field. Select forensic mailbox account associated with staff members.

BCC  ?

Scroll to the bottom of the screen and click on SAVE CHANGES. Complete similar setup for all communication tasks you would like to be running in a forensic mode.



Forensic mode takes effect instantly. If you are configuring live account, make sure e-mail boxes are configured and your server can receive large volume of e-mails.

---

🕒 Revision #9

★ Created Sat, Sep 21, 2019 7:47 PM by Dennis Ayzin

✎ Updated Tue, Aug 17, 2021 1:20 PM by manual admin