FORENSIC MODE

Deploy smart infrastructure and policies for outgoing communication.

- What is forensic mode of communication?
- Forensic mode infrastructure
- Implementing forensic mode

WHAT IS FORENSIC MODE OF COMMUNICATION?

ScheduleInterpreter® forensic mode of communication allows your organization to capture all outgoing messages initiated by the platform. These messages will include all information sent out to the requesters, clients, vendors and staff members. The messages will contain unique tags generated by the ScheduleInterpreter® mail server.

Use of forensic mode may require involvement of your IT and legal departments.

IT department of your organization will help with setting up the infrastructure for the forensic mode. The legal department will create policies defining how long correspondence shall be retained, access rights, audits and other legal requirements associated with compliance.

FORENSIC MODE INFRASTRUCTURE

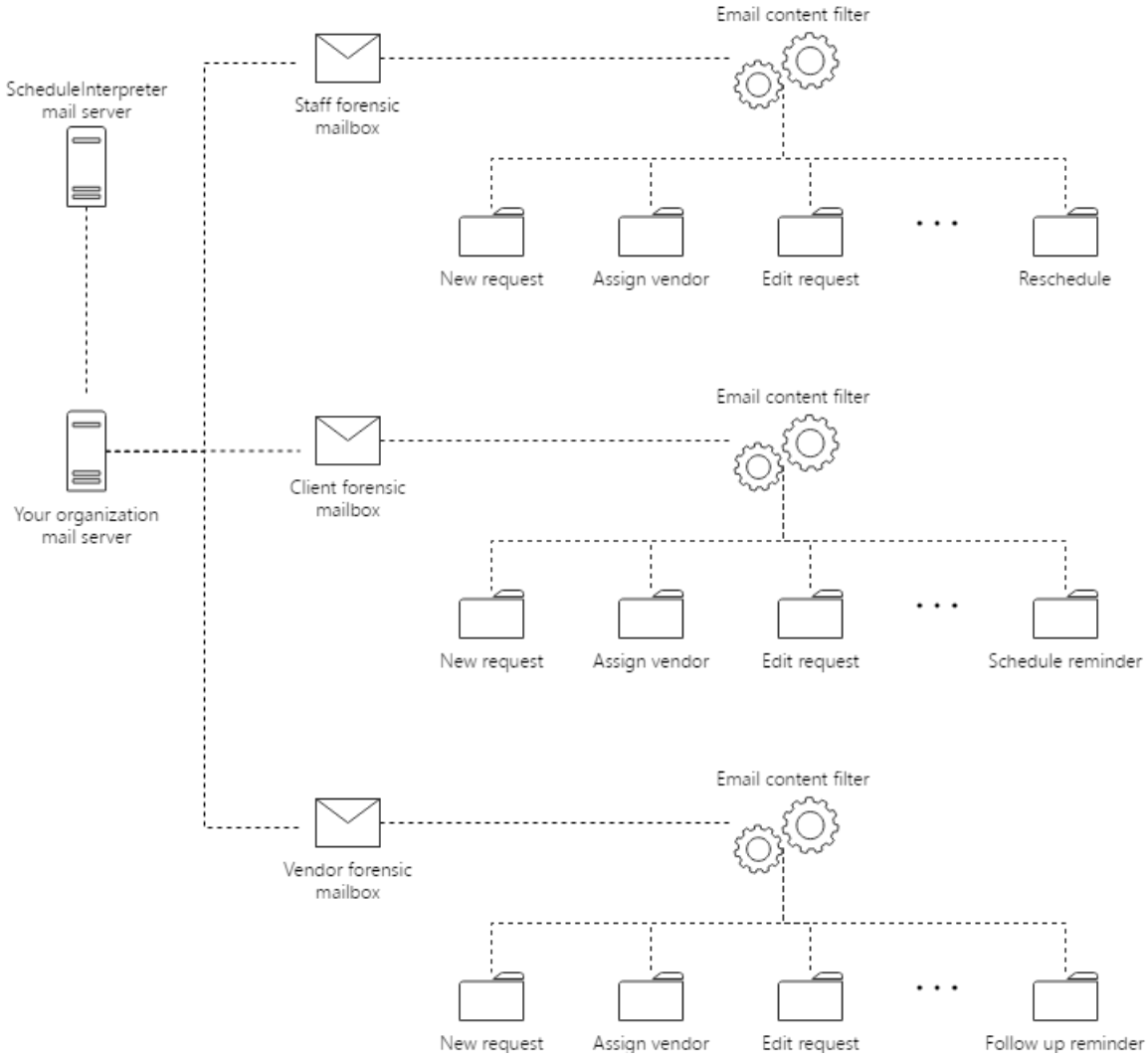
In forensic mode, all notifications can be categorized using the task notification was initiated by. For example, all new request notifications for vendors can be captured and stored separately from notifications sent to the staff members or requester.

MAILBOXES AND E-MAIL CONTENT FILTERS

Before deploying forensic mode the decision needs to be made if each category of notifications will have its own mailbox or all communication will be stored in a single mailbox with automated content filters. It is possible to deploy a hybrid solution using both features at the same time.

Making selection how the messages will be stored should be done before deployment of the forensic mode. Factors such as storage limits, retention policies and access right should be considered.

The diagram below provides an example for hybrid implementation of the forensic mode. This is the recommended form of the infrastructure for large organizations with no restrictions on storage. The structure allows capturing all messages and categorize them by the type of recipient. The filtered messages are then stored in separate folder.



IT department can assign access rights to the mailboxes that store the messages. More complex settings can be implemented with read only rights for a group of users within the organization.

RETENTION POLICY AND BACK UP

For majority of organization 7 years retention should be sufficient to meet most of the compliance requirements. With electronic storage costs constantly decreasing, retention limits can be removed completely.

Regular back up of the mailboxes should be part of the IT policy. Use of full and not incremental back up is recommended.

If storage restrictions exist, an automated policy of removal for messages older than retention period should be implemented. For compliance purpose, archived copies of the messages should be preserved.

HIPAA COMPLIANCE

Standard policies should be applicable for archived messages and storage. High-grade encryption and password protection are recommended.

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:

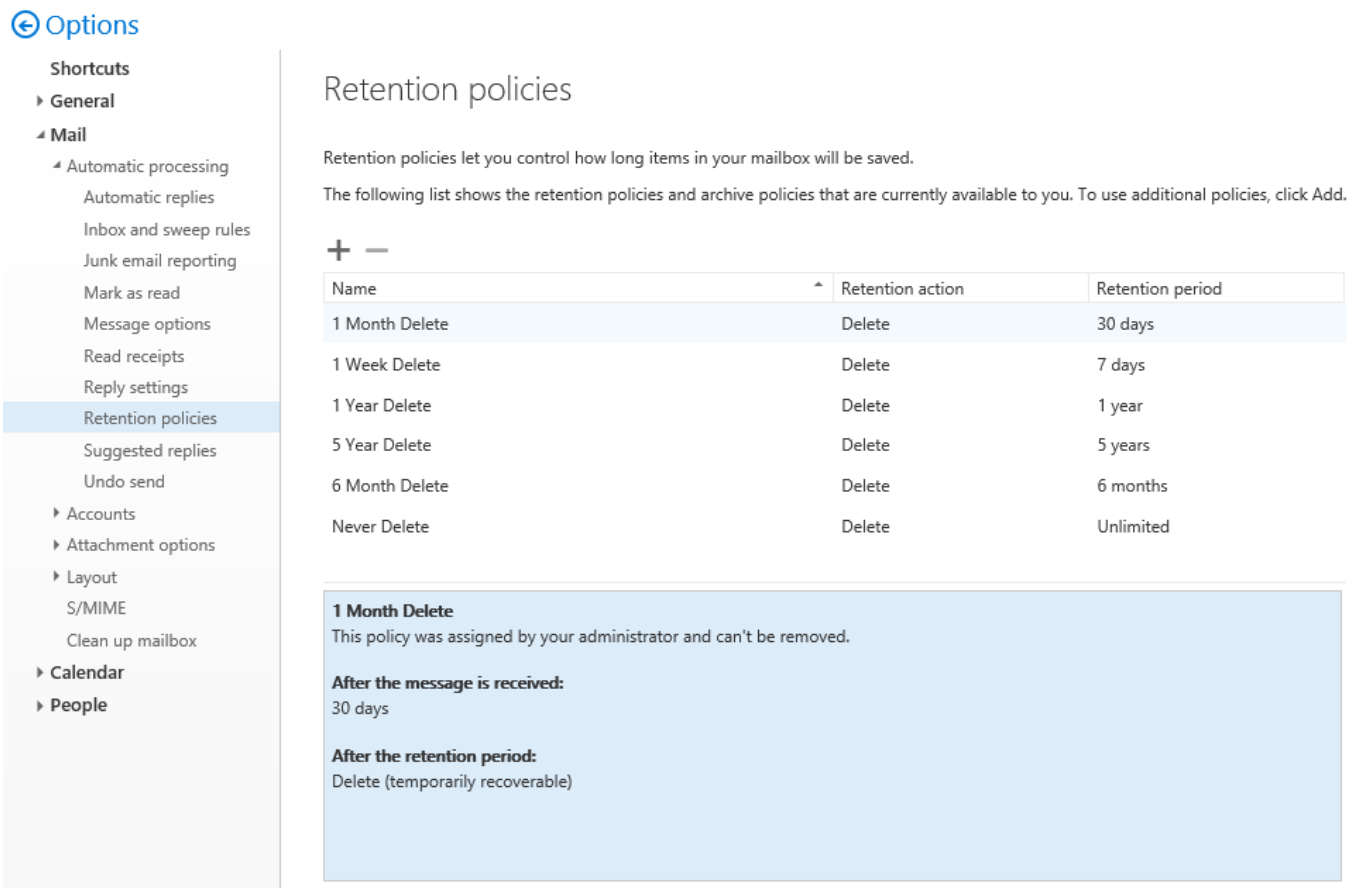
- forensic.staff@bestinterpreters.com - this mailbox will retain all internal communication initiated by ScheduleInterpreter®;
- forensic.client@bestinterpreters.com - this mailbox will retain all communication sent out by ScheduleInterpreter® to the requesters and administrative team of the account,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

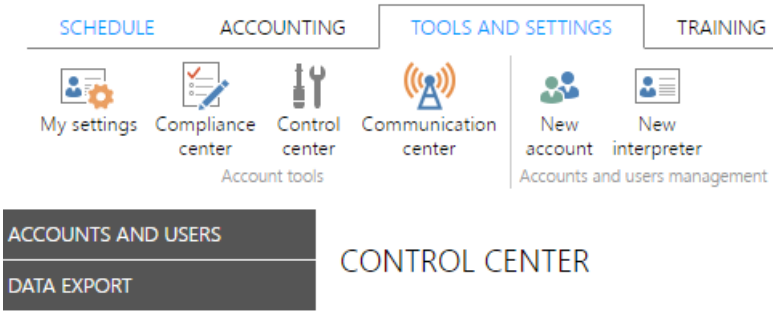
DEFINE RETENTION POLICIES

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.

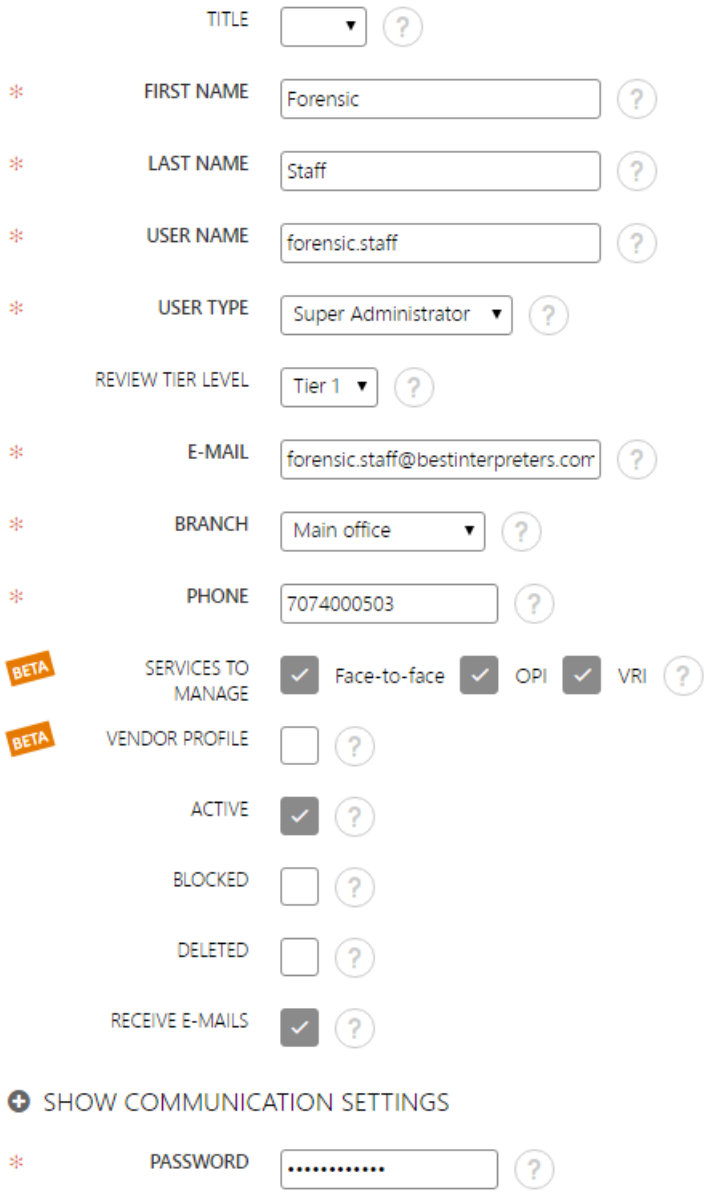


ADDING FORENSIC MAILBOXES TO YOUR ACCOUNT

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.



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.

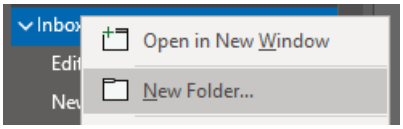
The process of creating robust filtering system will require planing of how the messages are going to be tagged. When implementing forensic mode, each message should include a unique tag. The simplest way is to include a tag into the body of the message. Most of the modern mail servers can read the content 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.

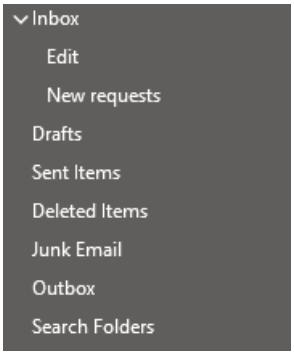
BUILD FILTERS

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.

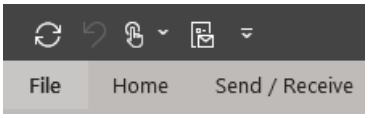


When place is created for a new folder enter New requests and hit Enter on your keyboard. Outlook will add the folder in a tree like structure, similar to the one shown below.

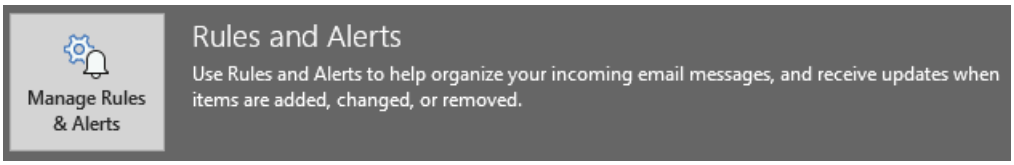


Add folders for each task from COMMUNICATION CENTER you would like to utilize forensic mode.

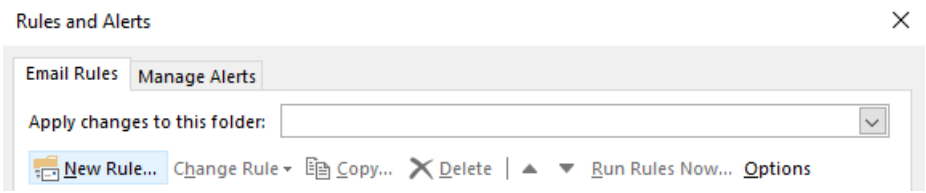
When all folders are added, use File menu to begin adding filters.



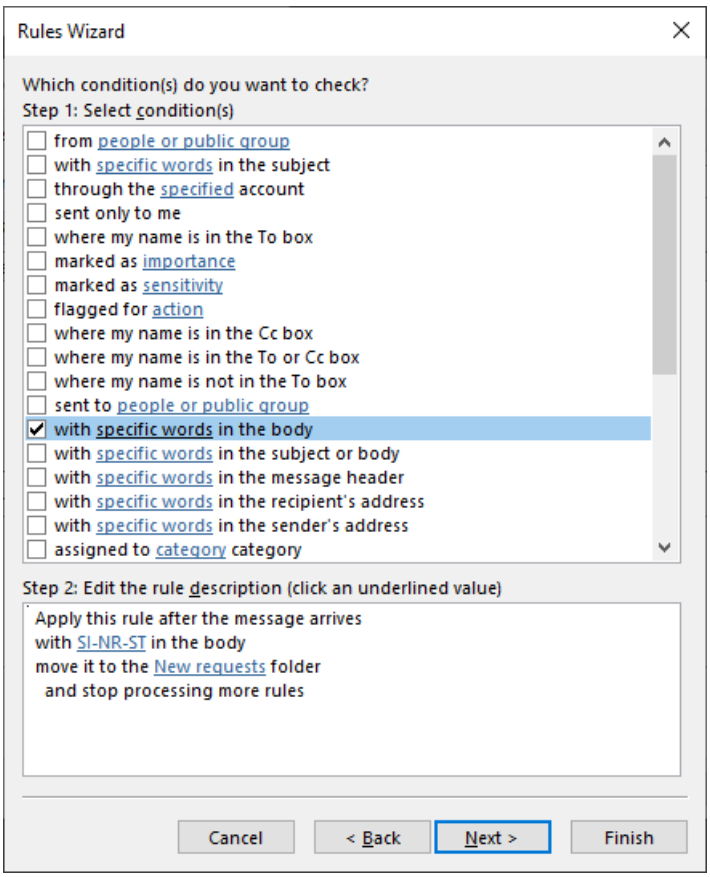
Locate and click on Rules and Alerts option



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



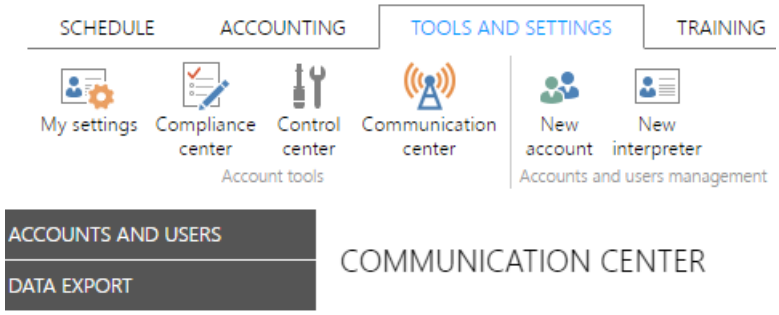
Complete configuration of the filter by selecting With specific words in the body and New requests in the folder. Your final selection should look like the one below.



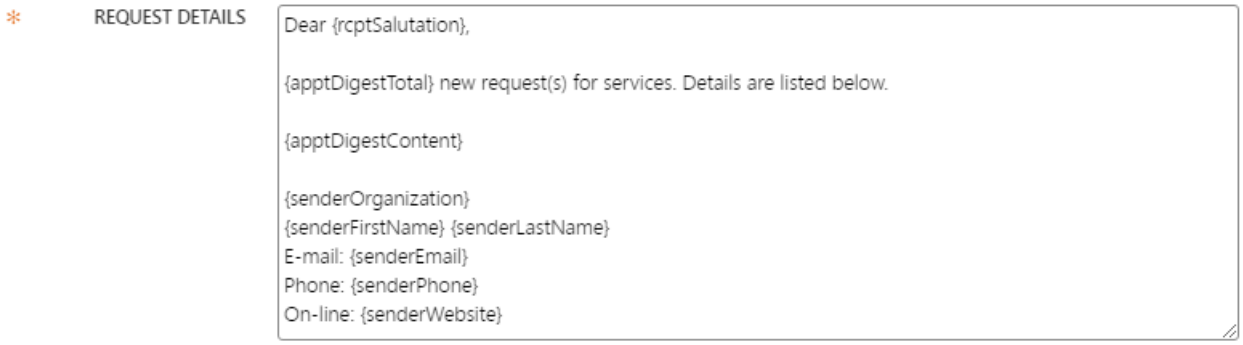
Click Next > button to fine tune your filter or click Finish button to complete the settings. Use similar steps to complete filters for all other tags. Identical process is needed for clients, vendors and consumers.

TAGGING MESSAGES

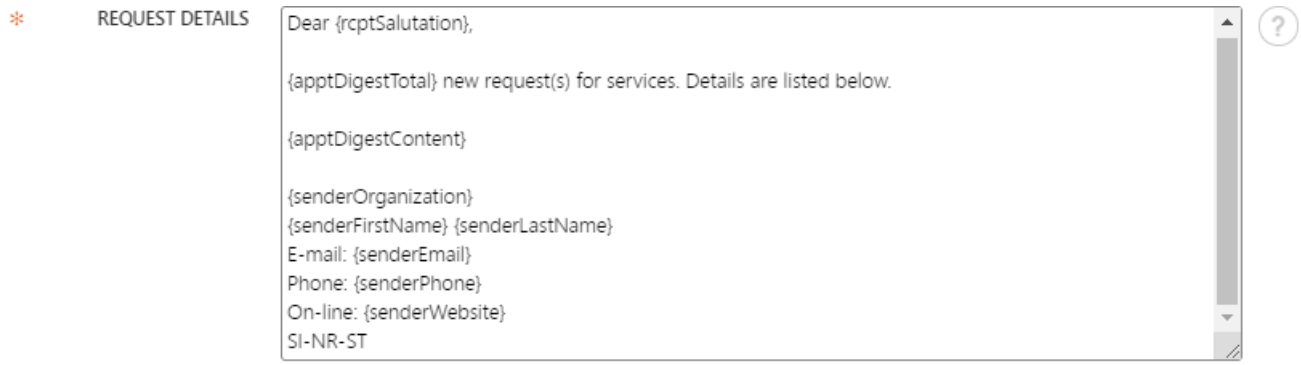
Login to your account in ScheduleInterpreter® with super administrator rights. Navigate to TOOLS AND SETTINGS > Communication center



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.



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



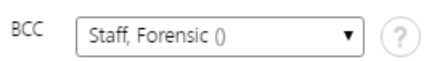
REQUEST DETAILS field is capable of accepting HTML content. You can minimize visibility of the tag by reducing the font size. Use following code to make the content of the tag smaller.

```
<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.



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.