# Threat Extraction Troubleshooting

## Introduction

The following is a collection of troubleshooting I need to do with Check Point Threat Extraction R80.10.

I used the Technical Reference Guide (ATRG) here: [sk114807](#)

### Workflow in MTA mode

1. A PostFix server receives and handles the emails.

2. Emails are forwarded to the *in.emaild.mta* daemon, which:
   1. Parses the emails (For example, Base64 decode)
   2. Passes the attachments to the *scrubd* process, if needed (based on the configuration of supported file types).

3. The *scrubd* process handles the file and sends it to the *scrub_cp_file_convertd* process with the relevant details (according to the policy).

4. *scrub_cp_file_convertd process*
   1. Converts the file / extracts potentialy malicious content from it.
   2. Returns a Safe copy of the file to *scrubd.*

5. The *scrubd* process returns the Safe copy to the *in.emaild.mta* daemon

6. The *in.emaild.mta* daemon:
   1. Replaces the original attachment with the Safe Copy version.

   2. Forwards the email to its destination.

**Note**: For environments with MTA bundle R80.10 jhf or R80.20, *in.emaild.mta* is replaced with *mtad* daemon

### Check log of convert to PDF process

It seems that the path is wron documented in the [sk114807](#)

The path mentioned **/var/log/jail/$FWDIR/log/scrub_cp_file_convertd.elg*** is in real **/var/log/jail/$CPMDIR/log/scrub_cp_file_convertd.elg***

## "This notification page has expired" error in UserCheck page when a user tries to download the original file that was blocked by Threat Extraction

**According to: [sk106249](sk106249)**

# Symptoms

**"This notification page has expired. You can safely close the page or" error in UserCheck page when a user tries to download the original attachment 7 days after receiving the original e-mail, although the Threat Extraction is configured to keep the original attachments for more than 7 days.**

[image-1614413932202.png](image-1614413932202.png)

- Attachment file still exists in /var/log/scrub/repository/ on Threat Extraction Gateway.
- The original mail can be retrieved by running the following command on the Security Gateway: scrub send_orig_email <email_id or reference_number> all.
- The Email ID or reference number can be retrieved from the incident log.

# Solution

For more information about the [sk106249](sk106249) you need to login to CP support portal. There you will need to check more files if you have set the "Delete stored original files older than" to 30+ days. These files ave been patched if you have installed the latest R80.10 Jumbo hotfixes.

The next SK mentioned is the following:

Persistence of UserCheck incidents is not preserved when quarantine time is very high

[sk122099](sk122099)

The solution for the SK above is to upgrade to R80.20

---

Revision #1
Created 27 February 2021 08:16:18
Updated 27 February 2021 08:20:51