In any cases, if you have any CSA questions on Cisco Unified CCX server, you may contact UCCX-Security team.

Before you contact UCCX-Security team, you may do the following:

1. Isolate the problem:

```
To confirm that your problem is CSA related, we highly recommend you to disable
CSA and replicate the problem.
To disable CSA from CLI, execute "utils csa disable".
Warning: a mandatory reboot is required.
```

2. Check for known defects [1]

3. Collect all CSA related logs:

```
To collect log from CLI, execute "utils create report csa" from CLI command,
this command should collect all the logs we need to diagnose the problem.
If the above CLI command is not available, you may collect CSA logs manually.
UCCX-Security team may request more logs, but in most cases, we only need
messages, csalog and securitylog.txt.
 To collect csalog: file get activelog syslog/csalog
 To collect securitylog: file get activelog syslog/securitylog
 To collect messages: file get activelog syslog/message
Provide the "core" file if available
If you suspect CSA driver induce kernel panic, try to take a snapshot of the screen/console.
Sometime it helps.
```

4. Contact UCCX-Security team with the following information:

```
1. Problem description
2. CUCM version
3. CSA version, this can be found out by any of the following commands:
   CLI: show packages active csa
   or, if root access is there then
   /opt/CSCOcsa/bin/csactl status
   or
   rpm -qa |grep csa
4. How to replicate the problem
5. Attach logs collected from step 3
```