Collecting Diagnostics and logs for Cyber Vision

Contents

Introduction

This document describes the steps required to collect logs on the Cyber Vision Solution. Cisco Cyber Vision has been specifically designed for industrial organizations to gain full visibility into their industrial networks, providing precise information on their OT security posture so they can build secure infrastructures, drive regulatory compliance, and enforce security policies to control risks.

Logs & Diagnostic files

From the Center CLI

1. To retrieve the sensors list and their IDs, type the command

```
sbs sensor list
```

2. To generate the diagnostic file, type the command

```
sbs diag
```

You can also use the 'sbs diag' command with other options depending on troubleshooting needs.

```
Available options:
  -f, --full     generate full statistics, very slow!
  -h, --help     this help message
  -o, --output   the path of the generated diagnostic (notice: archive will be generated at <path>.tgz)
  -v, --verbose  use verbose mode
```

â€f

3. To retrieve the logs for an enrolled sensor, type the command

```
sbs sensor log <sensor-ID>
```

From the Center GUI

Navigate to Administration â†' Sensors â†' Management & capture a screenshot. It would provide the connection, provisioning status along with the capture mode.

From the Sensor

1. On the sensor, from the Local Manager page in the GUI:
    a. System Info
    b. From the system Troubleshoot page, select â€œGenerate snapshot fileâ� then click â€œdownloadâ€�.

2. From the GUI, navigate to System statistics > Sensors > Generate Diagnostic, or from the CLI, use â€˜sbs diagâ€™.
    This will generate the diagnostics file under the /data/tmp/sbs-diag-export-<time stamp>.tgz directory.

3. From the CLI of the sensors (like IC3000), collect
    a. Show version
    b. Show interfaces
    c. Show iox summary