Troubleshooting Cisco NIA Application

This chapter contains the following sections:

Debugging Cisco NIA Application

Cisco NIA Application Start

The first login for Cisco NIA app takes some time for UI transition. The following message is displayed until application loads completely.

```
Please wait while Application data is being loaded.
```

Cisco NIA Application User Interface

- Most common user interface issues are due to receiving unexpected data from the APIs. Open the developer tools network tab and repeat the last action. It displays the API data received.
  - For issues with APIs, troubleshoot the backend logs.
  - For successful API requests and responses, check the developer tools console tab for errors, empty or unexpected data in the UI.
- After initial installation, the application needs time for UI transition and for complete loading. For any errors, take screenshots before and after reproducing an issue.
- Take a screenshot of full network capture saved as HAR from you browser. Open a service request and attach a HAR recording, backend logs, and screenshots for root cause analysis.

Statistics Telemetry

Statistics telemetry enables Cisco to collect statistics, inventory, and other telemetry information from customer networks. To debug statistics telemetry:

- Make sure that Device Connector is connected to Intersight cloud and claimed using the Device Connector user interface.
- Make sure that telemetry streaming is enabled. Check the check box for **Help Cisco improve its products**.

- Log into the compute node where the Device Connector is running.

```
# docker ps | grep "device \| intersight"
# docker exec it <dc container> bash
```

- In the logs directory, check the Device Connector logs for any failures related to inventory or etl update. Record the errors, collect Device Connector details, and collect Cisco NIA tech-support.

Advisory Report

Advisory report allows the user to export all advisory information from a link on the Advisories list view. To debug perform the following steps:

- From your browser tools page, right click Inspect, and click the network tab in your browser. Check if `/getAdvisoryReport` endpoint HTTP call status is successful.
- If the API call failed, view Active Data micro-service logs to check for any errors thrown in the micro-service. Collect Active Data micro-service logs for furthur analysis.

  If the API call is successful, but the file is not downloaded, check any popup blockers are enabled in the browser.

Debugging Software Upgrade Path

From your browser tools page, check if POST to *upgradepath* endpoint is successful and input or output data is as expected.

The following are the examples for *upgradepath*.

```
time="2020-01-22 07:43:59.485" level=info msg="new AdvMap=74522df14dfcas-UPG-admin"
file="upgradepath:204"
time="2020-01-22 07:43:59.485" level=info msg="Starting issumatrix call nxos 7.0(3)I7(1)
9.3(1)" file="upgradepath:277"
time="2020-01-22 07:43:59.485" level=info msg="Res output:[7.0(3)I7(1) 7.0(3)I7(5a) 9.3(1)]"
 file="upgradepath:297"
time="2020-01-22 07:43:59.486" level=info msg="Sending POST response" file="upgradepath:258"
```

Cisco APIC

```
time="2020-01-22 07:43:59.579" level=info msg="new AdvMap=s18sd3903s406sdssdbc-UPG-admin"
file="upgradepath:204"
time="2020-01-22 07:43:59.579" level=info msg="Starting issumatrix call aci 4.0(1) 4.2(3)"
 file="upgradepath:277"
time="2020-01-22 07:43:59.579" level=info msg="Res output:[4.0(1) 4.2(1) 4.2(3)]"
file="upgradepath:297"
time="2020-01-22 07:43:59.579" level=info msg="Init s18sd3903s406sdssdbc-UPG-admin{4.0(1)
4.2(1)}" file="upgradepath:216"
time="2020-01-22 07:43:59.579" level=info msg="Bugs output:map[4.2(1):0xc0004e2720
4.2(3):0xc0004e2780]" file="upgradepath:359"
time="2020-01-22 07:43:59.579" level=info msg="Sending POST response" file="upgradepath:258"
```

Notices

To debug notices:

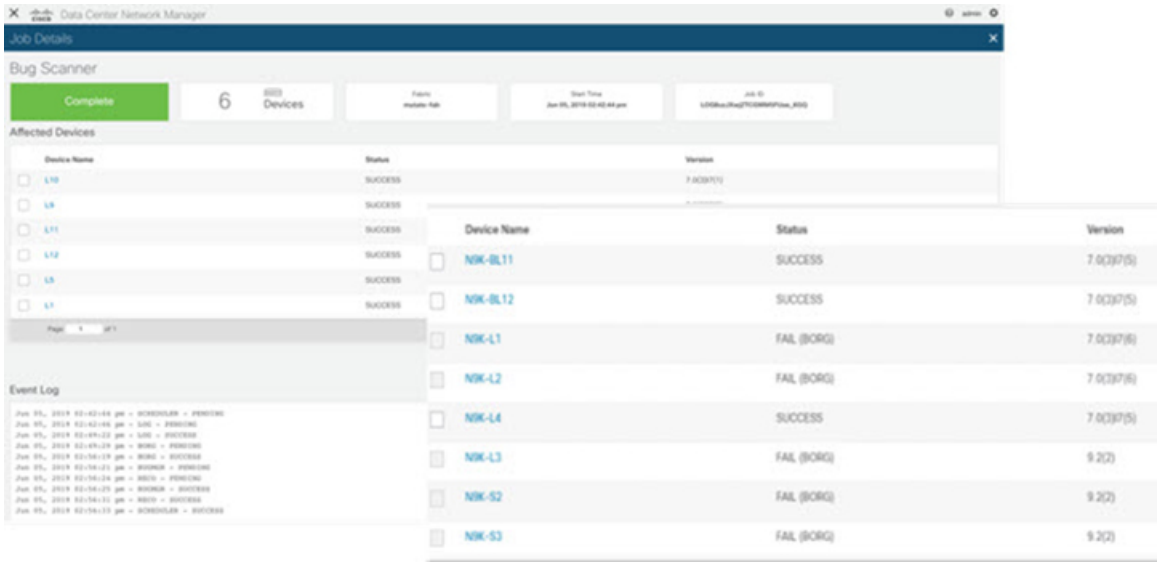
- Connect to the Intersight cloud and claim the Device Connector atleast once.
- Make sure that all the devices are available in the network.

- Make sure that all data is downloaded successfully.
- In case no notices appear, collect device connector details and collect Cisco NIA tech-support.

Bugs and PSIRTs

To debug for bug scan and PSIRTs:

- Connect to the Intersight cloud and claim the Device Connector atleast once.
- Make sure that all the devices are available in the network.
- Make sure that all metadata is downloaded successfully.
- Configure the on-demand bug scan.
- Check for the bug scan on-demand job progress.



- In the log archiver, check the tech-support logs collected from switch.
  - In case the logs are not collected, then collect infra tech-support.
  - In case the collected logs do not show the bugs, then collect Cisco NIA tech-support.

TAC Assist On-demand

To debug TAC assist on-demand job:

- Check the status of the job in the **Job List** page.
- In the log archiver, check that the logs are successfully collected from the switches.
- In the collected logs, check all the paths are reported for the logs.
- Collect the Cisco NIA tech-support in case of a failure.

Enhanced TAC Assist - User Initiated Upload to Cisco Cloud

In the user initiated TAC assist, the user collects the logs for specified devices and then uploads the collected logs to Cisco cloud. To debug perform the following steps:

- Make sure that Device Connector is connected to Intersight cloud and claimed using the Device Connector user interface.
- Log into the compute node where the Device Connector is running.

```
# docker ps | grep "device \| intersight"
# docker exec it <dc container> bash
```

- In the logs directory, check the Device Connector logs for any failures related to inventory or etl update. Record the errors, collect device connector details and collect Cisco NIA tech-support.

Example for uploading logs to Cisco cloud.

```
T22:05:35.087-0800 info stdplugins/techsupport.go:107
   Received request to collect techsupport for device: FDO22242J62, type: switch
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.087-0800 info  stdplugins/techsupport.go:166
   Invoking techsupport function.  {"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6",
"traceId": "PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.087-0800  info  niatech/techsupport.go:370
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.087-0800  info  niatech/techsupport.go:371     FDO22242J62
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
T22:05:35.122-0800  info  niatech/techsupport.go:339
         Got device model from dp
{"traceId": "AS0cb8885d3e0ad999ec14d74a5074cbd6", "traceId":
"PE98f043ee82967a1831f5a8c9eedfe25b"}
File start being uploaded:
T12:34:17.630-0800  info  niatech/techsupport.go:425
        Nashville: Finished techsupport collection with deviceType: switch, deviceId:
FDO22232LMZ
{"traceId": "ASc1a31b74ce56d39c3080fc97a4eba779", "traceId":
"PE0194accfee60ba13eee45ff21fa32b81"}
T12:34:17.630-0800  info  niatech/techsupport.go:426
             Nashville: Initiating techsupport upload with deviceType: switch, deviceId:
FDO22232LMZ
{"traceId": "ASc1a31b74ce56d39c3080fc97a4eba779", "traceId":
"PE0194accfee60ba13eee45ff21fa32b81"}
```

Cisco NIA Log Paths

Collect the logs to debug:

- Cisco APIC logs:
  - Within the container.

    ```
    /home/app/log/<microservice>
    ```
  - On each compute.

    ```
    /data2/logs/Cisco_NIA
    ```
  - Docker logs.

    ```
    /nomad logs –f <job_id>
    ```

- Collect Cisco NIA logs.

  Use tech-support policy for Cisco NIA application.

Troubleshooting Cisco NIA Application on Cisco APIC

Enhanced TAC Assist - TAC Initiated Pull from Cisco Cloud

The following table summarizes how to troubleshoot errors for Cisco TAC triggered on-demand collection of logs for specified devices, which were pulled from Cisco cloud.

Problem	Solution
The app returns a 404 error, "The serial number is not present in DP inventory" when triggering the technical support job.	• Make sure the device must be registered as endpoint in Device Connector. • Borgcore has a scheduler job to monitor the Device Connector claim change and devices change. After you claim the Device Connector or upload a newly added device, allow 5 minutes for Borgcore to detect the change and register correspondingly. After 5 minutes if the issue still exists, check Borgcore > techsupport log and check the registration log for errors.
The app returns an error, "NotFound" "The requested device is not registered in the system" when triggering fast-start job.	• Make sure the device you want to collect is registered in the same cloud. If the problem still persists, it could be due to duplicate claim of the same device. Intersight returns error if there is more than one device with the same serial number and PID combination. • Duplicate claim of the device can occur when Device Connector was unclaimed and claimed again without deleting the Device Connector from the Intersight UI. Unclaiming the Device Connector from UI will not delete the MO from the Intersight database.

Software Upgrade Path

The following table summerizes the troubleshooting scenarios for software upgrade path.

Problem	Solution
Unable to see an upgrade path after running bug scan or having a software EOL.	If bug scan or software EOL advisory displays “Contact Cisco Technical Assistance Center (TAC)” then upgrade path cannot be shown, since there is no target version to check against. Software version advisories are required to see an upgrade path, which shows the recommended version.
In the upgrade path link for two releases, multi-hop is displayed, but Cisco NIA displays single hop.	If an internal error occurs while calculating the upgrade path, Cisco NIA defaults to the single hop. See the section below for debugging upgrade path issues.
Newer version is not dispalyed in the recommended release or in the upgrade path.	• Check for the cloud connectivity and for the latest version of metadata. • If the latest version is available to run, then run metadata update and bug scan update.