Forcepoint Behavioral Analytics

3.4.1.2 UPGRADE GUIDE

Publish Date: October 11, 2022

F23-10-03-00

Legal Notice

Attributions

Document Conventions

The following typographic conventions are used in this guide:

Typography

Format	Description
Bold font	Used to identify Graphical User Interface (GUI) elements, buttons, fields, and list labels. Example: Type your IP address in the **ip address** field and click **OK**.
Italic font	Used to identify book titles or words that require emphasis. Example: Read the *User's Guide.*
Monospaced font	Used to identify names of commands, files, and directories. Example: Use the `ls -a` command to list all files.
Monospaced bold font	When inline, this is used to identify text that users need to type. Example: Type **`SYSTEMHIGH`** in the **Network** field.
Shaded monospaced font	Used to identify screen output. Example: A network device must exist; otherwise, the following warning message displays `Warning: device [DEVICE] is not a valid network device`
Shaded monospaced bold font	Used to identify text that users need to type. Example: Specify your network configuration. Type: **`$ sudo ip addr show`**

This guide makes use of the following elements:

Note
Contains important information, suggestions or references to material covered elsewhere in the guide.

Tip
Provides helpful suggestions or alternative methods to perform a task.

Warning
Alerts you to an activity that may cause permanent loss of data or product functionality. Failure to heed a warning could result in permanent consequences to your data or system.

Caution
Alerts you to anything that could result in a security breach or temporary loss of data or product functionality. You may also see a caution when a particular action may have an adverse impact that is not readily apparent.

Important
Highlights critical tasks, information or actions that may be damaging to your system or security.

CONTENTS

Upgrade Guide for Forcepoint Behavioral Analytics Hotfix (3.4.1.2)

To begin the hotfix upgrade, download the hotfix file package for the version of the environment that is being patched. The package consists of the FBA service jar files that have been upgraded with the Log4j v2.17.1 package:

- FBA 3.4.1: Forcepoint Behavioral Analytics 3.4.1.2 Hotfix

Note
When applying the hotfix to 3.4.0 or any containerized install, the following changes should be performed within the Docker containers.

The hotfix download package consists of the following files:

- Jenkins Service:
  - `ro-schema.jar`
  - `minigator.jar`
  - `ro-pst-parser.jar`
- Public API Service: `ro-api.jar`
- Content Service: `ro-content.jar`
- Conversion Service: `ro-conv.jar`
- Queue Worker Service: `ro-qw.jar`
- Rose Service: `ro-rose.jar`
- Master Data Service: `ro-mds.jar`

Default location of jar files on each server:

- API server: `/usr/lib/java/ro-api/ro-api.jar`
- Content server: `/usr/lib/java/ro-content/ro-content.jar`
- Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar`
- Jenkins server:
  - `/usr/lib/java/ro-schema/ro-schema.jar`
  - minigator and pst-parser are not installed by default.
- QW server: `/usr/lib/java/ro-qw/ro-qw.jar`
- Rose server: `/usr/lib/java/ro-rose/ro-rose.jar`
- MDS server: `/usr/lib/java/ro-mds/ro-mds.jar`
- MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar`

All steps below are performed on various FBA java services

1. Copy the service jar file to its respective hosts via scp or other means. For instance, the `ro-mds.jar` file should be copied to the `MDS` and `MDSLytics` hosts.

```
#scp example
scp ro-mds.jar user@mds-yourenvironment:/home/user/ro-mds.jar
scp ro-mds.jar user@mdslytics-yourenvironment:/home/user/ro-mds.jar
```

2. Stop the respective host services. For instance, stopping the MDS service on both on the MDS and MDSLytics hosts.

```
#example
ssh -l user mds-yourenvironment
sudo service ro-mds stop
ssh -l user mdslytics-yourenvironment
sudo service ro-mds stop
```

3. Rename the original service jar files as a backup.

```
#example
cd /usr/lib/java/ro-mds
sudo mv ro-mds.jar ro-mds.original
```

4. Move the new jar file into the appropriate file location.

```
#example
sudo mv /home/user/ro-mds.jar /usr/lib/java/ro-mds/ro-mds.jar
```

5. Start the service being upgraded.

```
#example
sudo systemctl start ro-mds
```

6. Repeat steps 3 through 7 for the 7 FBA services listed above
7. Ensure the fix is working as expected.
8. If a rollback is required, perform the following steps on each of the patched service hosts:
   a. Stop the service such as `sudo systemctl ro-mds stop`
   b. Rename the existing service jar file by replacing the word jar with ***xyz patch version***hotfix.

```
Example:
sudo mv ro-mds.jar ro-mds.3313hotfix
```

   c. Rename backup jar file by replacing the word original in file name to jar.

```
Example:
sudo mv ro-mds.original ro-mds.jar
```

   d. Start the service.

```
Example:
sudo systemctl ro-mds start
```

e. Ensure the product is working as expected.