

# Forcepoint Behavioral Analytics

## 3.4.1.2 UPGRADE GUIDE

THESE ITEMS ARE CONTROLLED BY THE U.S. GOVERNMENT AND AUTHORIZED FOR EXPORT ONLY TO THE COUNTRY OF ULTIMATE DESTINATION FOR USE BY THE ULTIMATE CONSIGNEE OR END-USER(S). THEY MAY NOT BE RESOLD, TRANSFERRED, OR OTHERWISE DISPOSED OF, TO ANY OTHER COUNTRY OR TO ANY PERSON OTHER THAN THE AUTHORIZED ULTIMATE CONSIGNEE OR END-USER(S), EITHER IN THEIR ORIGINAL FORM OR AFTER BEING INCORPORATED INTO OTHER ITEMS, WITHOUT FIRST OBTAINING APPROVAL FROM THE U.S. GOVERNMENT OR AS OTHERWISE AUTHORIZED BY U.S. LAW AND REGULATIONS.

PROPRIETARY

Publish Date: October 11, 2022

Copyright © 2022

F23-10-03-00

## Legal Notice

No part of this document shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the company. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this document, the authors and the company assume no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or completeness is implied. The provided information is on an "as is" basis. The authors and the company shall have neither liability nor responsibility for any loss or damages arising from the information contained in this document. Printed in the United States of America.

**This document contains proprietary information and is furnished for evaluation purposes only, and, except with written permission of the vendor, such information shall not be published, or disclosed to others, or used for any other purpose, or duplicated in whole or in part.**

## Attributions

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. The company cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

## 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 <b>ip address</b> field and click <b>OK</b> .
Italic font	Used to identify book titles or words that require emphasis. Example: Read the <i>User's Guide</i> .
Monospaced font	Used to identify names of commands, files, and directories. Example: Use the <code>ls -a</code> command to list all files.
Monospaced bold font	When inline, this is used to identify text that users need to type. Example: Type <b>SYSTEMHIGH</b> in the <b>Network</b> field.
Shaded monospaced font	Used to identify screen output. Example: A network device must exist; otherwise, the following warning message displays <div>Warning: device [DEVICE] is not a valid network device</div>
Shaded monospaced bold font	Used to identify text that users need to type. Example: Specify your network configuration. Type: <div><b>\$ sudo ip addr show</b></div>

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) .....	5
--	---

THIS ITEM IS SUBJECT TO THE EXPORT CONTROL LAWS OF THE U.S. GOVERNMENT. EXPORT, RE-EXPORT OR TRANSFER CONTRARY TO THOSE LAWS IS PROHIBITED.

# 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.