# Forcepoint Behavioral Analytics

## FBA 3.4.2.XX PATCH INSTRUCTIONS

**WARNING**: THIS DOCUMENT IS SUBJECT TO THE EAR (U.S. EXPORT ADMINISTRATION REGULATIONS 15 C.F.R. §730-774) AND CONTAINS TECHNOLOGY WHOSE EXPORT OR DISCLOSURE MUST BE IN ACCORDANCE WITH THE EAR. VIOLATIONS ARE SUBJECT TO PENALTIES.

FORCEPOINT PROPRIETARY

Publish Date: February 12, 2024

F23-09-06-00

## 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is furnished for evaluation purposes only, and, except with written permission of the vendor, such information shall not be published, or disclosed to others, or used for any other purpose, or duplicated in whole or in part.**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.<br>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.<br>Example: Read the *User's Guide*. |
| Monospaced font | Used to identify names of commands, files, and directories.<br>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.<br>Example: Type **`SYSTEMHIGH`** in the **Network** field. |
| Shaded monospaced font | Used to identify screen output.<br>Example: A network device must exist; otherwise, the following warning message displays<br>`Warning: device [DEVICE] is not a valid network device` |
| Shaded monospaced bold font | Used to identify text that users need to type.<br>Example: Specify your network configuration. Type:<br>**`$ 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

# FBA 3.4.2.x Patch Update Instructions

This Forcepoint Behavioral Analytics (FBA) Upgrade manual will guide technical FBA users through a complete patch upgrade from version 3.4.2 to the latest version 3.4.2.xxx of the FBA system. This guide includes instructions for an automated upgrade that will result in a fully functional 3.4.2.xxx system when complete.

**Note**
Replace the term 'xxx' with the number digit for the hotfix patch (*for example*: for the first patch, term 3.4.2.xxx should become 3.4.2.1 and 3.4.2.xxx should become 3.4.2.1 in these instructions )

For Limited Availability ("rootless & containerized") installs, these changes need to be performed within the Docker containers so require the following port details added to the commands. For a containerized solution, perform the following replacements:

```
From: <SCP_PORT> To: -P 2222
From: <SSH_PORT> To: -p 2222
```

For General Availability ("non-containerized") installs, perform the following changes to the instructions:

```
Remove <SCP_PORT>
Remove <SSH_PORT>
```

## AUTOMATED INSTALLATION INSTRUCTIONS

1. Download the Forcepoint Behavioral Analytics version 3.4.2.xxx Patch file.

   **Note**
   The hotfix file package can be found in the "*Hotfix*" section of the download page.

2. Upload the hotfix file package to the Jenkins host:

   ```
   scp [-i ~/.ssh/my.pem] <SCP_PORT> fba-patch-3.4.2.xxx.tar [Jenkins-server]:/tmp/
   ```

3. Log in to the Jenkins host and extract the patch files:

   ```
   ssh [-i ~/.ssh/my.pem] <SSH_PORT> centos@[Jenkins-server]

   sudo tar -xvf /tmp/fba-patch-3.4.2.xxx.tar -C /data/html/
   ```

4. Run the Ansible® playbook:

   ```
   cd /data/html/patch-3.4.2.xxx/ansible
   ansible-playbook FBA-patch-installer.yml -i /etc/ansible/hosts

   curl -k -u elastic:changeme -XPUT "https://<ES1-SERVER>:9200/_cluster/settings" -
   d'{"transient": {"cluster.routing.allocation.enable": "all"}}'
   ```

**Note**
If authentication errors occur, ensure that the logged in user is the Centos™ user, If errors persist, disable host key checking:

```
vim /etc/ansible/ansible.cfg
HOST_KEY_CHECKING = False
```

**Important**
Any custom UI changes must be applied manually. Custom changes will not persist to the new version.

5. Remove backup files that were created during install to ensure that all files with the old versions of Log4j™ library code are removed. The following locations will have backup files:

   API server: `/usr/lib/java/ro-api/ro-api.jar.pre3.4.2.xxx`

   Content server: `/usr/lib/java/ro-content/ro-content.jar.pre3.4.2.xxx`

   Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar.pre3.4.2.xxx`

   Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar.pre3.4.2.xxx`

   Nifi server:`/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar.pre3.4.2.xxx`

   QW server: `/usr/lib/java/ro-qw/ro-qw.jar.pre3.4.2.xxx`

   Rose server: `/usr/lib/java/ro-rose/ro-rose.jar.pre3.4.2.xxx`

   MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.xxx`

   MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.xxx`

   UI server: `/data/patch-3.4.2.xxx-backup/ro-ui.backup.tar`

## INSTALLATION BACKOUT

1. Replace the 3.4.2.xxx `.jar` files with the original `.jar` files. The `.jar` file are located in the following locations:

```
API <FBA SERVICE>: ro-api
Content <FBA SERVICE>: ro-content
Conversion <FBA SERVICE>: ro-conv  (sometimes there is more than 1 conversion
services, update the name accordingly)
Jenkins <FBA SERVICE>: ro-schema
Nifi <FBA SERVICE>: ro-ingest-utils
QW <FBA SERVICE>: ro-qw  (sometimes there is more than 1 queue worker services,
update the name accordingly)
Rose <FBA SERVICE>: ro-rose
MDS / MDSLYTICS <FBA SERVICE>: ro-mds   (sometimes there is more than 1 mds
services so you may need to update name accordingly)
```

```
sudo systemctl stop <FBA SERVICE>
cd /usr/lib/java/<FBA SERVICE>
sudo rm /usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar
sudo mv /usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.pre3.4.2.xxx /usr/lib/java/<FBA
SERVICE>/<FBA SERVICE>.jar
sudo systemctl start <FBA SERVICE>
```

2. Back out UI changes.
3. Extract the backup patch installer that was created:

```
sudo tar -xvf /data/patch-3.4.2.xxx-backup/ro-ui.backup.tar -C /usr/lib/node_
modules/ro-ui/
```

4. Other Servers:

```
# Re-deploy via Jenkins job.

build deploy elastic

build deploy logstash

build deploy monitoring

build deploy kafka
```