Forcepoint Behavioral Analytics

3.4.2.2 UPGRADE GUIDE

Publish Date: December 29, 2022

F23-09-03-01

Legal Notice

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is furnished for evaluation purposes only, and, except with written permission of the vendor, such information shall not be published, or disclosed to others, or used for any other purpose, or duplicated in whole or in part.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

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.

Forcepoint Behavioral Analytics 3.4.2.2 Upgrade Guide

This Forcepoint Behavioral Analytics (FBA) Upgrade manual will guide technical FBA users through a complete upgrade from version 3.4.2 to the latest version 3.4.2.2 of the FBA system. This guide includes instructions for an automated upgrade and instructions for a manual upgrade that will result in a fully functional 3.4.2.2 system when complete.

To update a Limited Availability 3.4.2 environment (rootless & containerized) port details must be added to the commands and must be performed within the Docker containers:

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

To update a General Availability 3.4.2 environment (non-containerized) perform the following changes to instructions:

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

Tip
For best results using the copy and paste function for the commands in this guide, this document should be viewed in an external pdf viewer.

AUTOMATED INSTALLATION INSTRUCTIONS

1. Download the Forcepoint Behavioral Analytics version 3.4.2.2 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-3.4.2.2.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-3.4.2.2.tar -C /data/html/
   ```

4. Run the Ansible® playbook:

   ```
   cd /data/html/patch-3.4.2.2/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. Forcepoint will not persist those changes 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:

   MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.2`

   MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.2`

   UI server: `/data/patch-3.4.2.2-backup/ro-ui.backup.tar`

INSTALLATION BACKOUT

1. Replace the 3.4.2.2 `.jar` files with the original `.jar` files. The `.jar` file are located in the following locations:

   # Pre-Patch Versions

   MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.2`

   MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.2`

   # Destination

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

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

```
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>.pre3.4.2.2 /usr/lib/java/<FBA
SERVICE>/<FBA SERVICE>.jar
sudo systemctl start <FBA SERVICE>
```

2. Back out UI changes.

   Tip
   After backing out the UI changes, performing one of the following options is suggested:

   Option 1:

   - Redeploy the UI via Jenkins job.
   - Apply any UI patch that ay have been introduced.

   Option 2:

   - Extract the backup the patch installer created:

```
sudo tar -xvf /data/patch-3.4.2.2-backup/ro-ui.backup.tar -C
/usr/lib/node_modules/ro-ui/
```

3. Other Servers:

```
# Re-deploy via Jenkins job.
build deploy elastic
build deploy logstash
build deploy monitoring
build deploy kafka
```