Forcepoint Behavioral Analytics

3.4.2.3 UPGRADE GUIDE

Publish Date: June 08, 2023

F23-09-04-00

Legal Notice

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

Forcepoint Behavioral Analytics 3.4.2.3 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 patch version 3.4.2.3 of the FBA system. This guide includes instructions for an automated upgrade that will result in a fully functional 3.4.2.3 system when complete.

AUTOMATED INSTALLATION INSTRUCTIONS

Important
For Limited Availability ("rootless & containerized") installs, these changes must be performed within the Docker containers. The following port details must be 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-conatainerized") installs, perform the following changes to the instructions:

```
Remove <SCP_PORT>

Remove <SSH_PORT>
```

1. Download the 3.4.2.3 hotfix patch file.

   Note
   The patch file package can be found in the "Hotfix" section of the Forcepoint Downloads page.

2. Upload the Patch `.tar` file to the Jenkins host:

   ```
   scp [-i ~/.ssh/my.pem] <SCP_PORT> fba-patch-3.4.2.3.tar [Jenkins-server]:/tmp/
   ```

3. Log in to the Jenkins host with the standard login used to run Ansible®, and extract the patch files:

   Tip
   Replace `<centos>` in the example below, with the standard ID.

   ```
   ssh [-i ~/.ssh/my.pem] <SSH_PORT> centos@[Jenkins-server]
   sudo tar -xvf /tmp/fba-patch-3.4.2.3.tar -C /data/html/
   ```

4. Run the Ansible playbook:

```
cd /data/html/patch-3.4.2.3/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"}}'
```

Tip
If authentication errors occur, ensure that the logged in user is the Centos™ user. If the errors continue, disable host key checking:

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

5. Apply any custom UI changes.

Note
These are changes that are not provided by Forcepoint and included with the FBA application.

6. Confirm that the new version of FBA is functioning as expected.
7. 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.pre3423`

   Content server: `/usr/lib/java/ro-content/ro-content.jar.pre3423`

   Conversion server: `/usr/lib/java/ro-conv/ro-conv.jar.pre3423`

   Jenkins server: `/usr/lib/java/ro-schema/ro-schema.jar.pre3423`

   Nifi server: `/usr/share/java/ro-ingest-utils/ro-ingest-utils.jar.pre3423`

   QW server: `/usr/lib/java/ro-qw/ro-qw.jar.pre3423`

   Rose server: `/usr/lib/java/ro-rose/ro-rose.jar.pre3423`

   MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3423`

   MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3423`

   UI server: `/data/patch-3.4.0.3-backup/ro-ui.backup.tar`

INSTALLATION BACKOUT

1. Replace patched version of the FBA service `.jar` file with the original `.jar` file in each environment.

   The hosts and locations of the jar files that must be updated are located here:

   API <FBA SERVICE>: `ro-api`

   Content <FBA SERVICE>: `ro-content`

   Conversion <FBA SERVICE>: `ro-conv`

   Note
   There may be more than one conversion service. All services must be updated.

   Jenkins <FBA SERVICE>: `ro-schema`

   Nifi <FBA SERVICE>: `ro-ingest-utils`

   QW <FBA SERVICE>: `ro-qw`

   Note
   There may be more than one que worker service. All services must be updated.

   Rose <FBA SERVICE>: `ro-rose`

   MDS / MDSLYTICS <FBA SERVICE>: `ro-mds`

   Note
   There may be more than one MDS service. All services must be updated.

2. Stop the FBA service:

```
sudo systemctl stop <FBA SERVICE>
```

3. Change directories to the FBA service that is to be backed out:

```
cd /usr/lib/java/<FBA SERVICE>
```

4. Replace the new `.jar` file with the old `.jar` file:

```
sudo rm /usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar
sudo mv /usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar.pre3.4.2.3
/usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar
```

5. Restart the FBA Services:

```
sudo systemctl start <FBA SERVICE>
```

Note
Repeat steps 2-5 for each FBA service.

6. Back out UI changes.

Tip
Reverting the UI to the backup version is recommended:

```
sudo tar -xvf /data/patch-3.4.2.3-backup/ro-ui.backup.tar -C /usr/lib/node_
modules/ro-ui/
```

7. Redeploy the other servers using Jenkins:

   build deploy elastic

   build deploy logstash

   build deploy monitoring

   build deploy kafka