Forcepoint Behavioral Analytics

3.4.2.1 UPGRADE GUIDE

Publish Date: January 09, 2023

F23-09-05-00

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

Forcepoint Behavioral Analytics 3.4.2.1 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 3.4.2.1 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 3.4.2.1 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 3.4.2.1 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-3.4.2.1.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-3.4.2.1.tar -C /data/html/
   ```

4. Run the Ansible® playbook:

   ```
   cd /data/html/patch-3.4.2.1/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.pre3.4.2.1`

   MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.1`

   UI server: `/data/patch-3.4.2.1-backup/ro-ui.backup.tar`

MANUAL INSTALLATION INSTRUCTIONS

1. Download the Forcepoint Behavioral Analytics version 3.4.2.1 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-3.4.2.1.tar [Jenkins-server]:/tmp/
   ```

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

   ```
   scp [-i ~/.ssh/my.pem] <SCP_PORT> fba-patch-3.4.2.1.tar [Jenkins-server]:/tmp/
   ```

4. Copy the `.tar` file from the Jenkins server to the Elasticsearch®, Monitoring, and Kafka™

   Note
   The `[server]` value in the commands below must be replaced with the names of the Elasticsearch, Monitoring, and Kafka names in the FBA environment.

   ```
   scp [-i ~/.ssh/my.pem] <SCP_PORT> /tmp/fba-patch-3.4.2.1.tar [server]:/tmp/
   ssh [-i ~/.ssh/my.pem] <SSH_PORT> centos@[server] tar -xvf /tmp/fba-patch-
   3.4.2.1.tar -C /tmp/
   ```

5. Shut down the necessary services on each of the environments associated with Elasticsearch and Monitoring to allow for the Log4j updates to Elasticsearch:

```
sudo systemctl status [server]_elasticsearch.service
sudo systemctl stop [server]_elasticsearch.service
sudo systemctl status [server]_elasticsearch.service

sudo rm /usr/share/elasticsearch/lib/log4j-*
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/share/elasticsearch/lib/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-1.2-api-2.18.0.jar
/usr/share/elasticsearch/lib/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
/usr/share/elasticsearch/lib/
sudo chown root:root /usr/share/elasticsearch/lib/log4j-*
sudo chmod 644 /usr/share/elasticsearch/lib/log4j-*
```

6. Shut down the necessary services on each of the environments associated with UI, Elasticsearch, and Monitoring to allow for the Log4j updates to Logstash:

```
sudo systemctl status logstash.service
sudo systemctl stop logstash.service
sudo systemctl status logstash.service

sudo rm /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
api/2.6.2/log4j-api-2.6.2.jar
sudo rmdir /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
api/2.6.2
sudo mkdir /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
api/2.18.0
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chown -R logstash:logstash /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chmod 755 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chmod 664 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-api/2.18.0/log4j-api-2.18.0.jar

sudo rm /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
core/2.6.2/log4j-core-2.6.2.jar
sudo rmdir /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
core/2.6.2
sudo mkdir /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
core/2.18.0
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
/usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
```

```
core/2.18.0/sudo chown -R logstash:logstash /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/
sudo chmod 755 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/
sudo chmod 664 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-core/2.18.0/log4j-core-2.18.0.jar

sudo rm /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
slf4j-impl/2.6.2/log4j-slf4j-impl-2.6.2.jar
sudo rmdir /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
slf4j-impl/2.6.2
sudo mkdir /usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-
slf4j-impl/2.18.0
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-slf4j-impl-2.18.0.jar
/usr/share/logstash/logstash-core/lib/org/apache/logging/log4j/log4j-slf4j-
impl/2.18.0/
sudo chown -R logstash:logstash /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0/
sudo chmod 755 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0/
sudo chmod 664 /usr/share/logstash/logstash-
core/lib/org/apache/logging/log4j/log4j-slf4j-impl/2.18.0/log4j-slf4j-impl-
2.18.0.jar


sudo rm /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-
3.1.3-java/vendor/jar-dependencies/runtime-jars/log4j-1.2.17.jar
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-1.2-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-3.1.3-
java/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-3.1.3-
java/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-3.1.3-
java/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-3.1.3-
java/vendor/jar-dependencies/runtime-jars/log4j-1.2-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-3.1.3-
java/vendor/jar-dependencies/runtime-jars/log4j-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-log4j-3.1.3-
java/vendor/jar-dependencies/runtime-jars/log4j-core-2.18.0.jar
sudo chmod 644 /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-
log4j-3.1.3-java/vendor/jar-dependencies/runtime-jars/log4j-*
```

```
sudo rm /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-1.2.17.jar
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-1.2-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-1.2-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-api-2.18.0.jar
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-core-2.18.0.jar
sudo chmod 644 /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-output-
kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-*

sudo rm /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-beats-
3.1.32-java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-
api/2.6.2/log4j-api-2.6.2.jar
sudo rmdir /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-beats-
3.1.32-java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-api/2.6.2
sudo mkdir /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-beats-
3.1.32-java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-api/2.18.0
sudo cp /tmp/apache-log4j-2.18.0-bin/log4j-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-beats-3.1.32-
java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chown -R logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-beats-3.1.32-
java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-api/2.18.0/
sudo chmod 755 /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-
beats-3.1.32-java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-
api/2.18.0
sudo chmod 644 /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-
beats-3.1.32-java/vendor/jar-dependencies/org/apache/logging/log4j/log4j-
api/2.18.0/log4j-api-2.18.0.jar

sudo rm /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-slf4j-impl-2.8.2.jar
sudo cp /tmp/apache-log4j-2.18.0-bin/log4j-slf4j-impl-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-kafka-
```

```
5.1.11/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-slf4j-impl-2.18.0.jar
sudo chmod 664 /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-
kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-slf4j-impl-2.18.0.jar

sudo rm /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-api-2.8.2.jar
sudo cp /tmp/apache-log4j-2.18.0-bin/log4j-api-2.18.0.jar
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/
sudo chown logstash:logstash
/usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-kafka-
5.1.11/vendor/jar-dependencies/runtime-jars/log4j-api-2.18.0.jar
sudo chmod 664 /usr/share/logstash/vendor/bundle/jruby/1.9/gems/logstash-input-
kafka-5.1.11/vendor/jar-dependencies/runtime-jars/log4j-api-2.18.0.jar

grep -Rl "log4j-api" /usr/share/logstash/* | xargs sudo sed -i
's/2\.6\.2/2\.18\.0/g'
```

7. Restart the processes for Elasticsearch:

```
sudo systemctl status [server]_elasticsearch.service
sudo systemctl start [server]_elasticsearch.service
sudo systemctl status [server]_elasticsearch.service
```

8. Restart the Logstash services:

```
sudo systemctl status logstash.service
sudo systemctl start logstash.service
sudo systemctl status logstash.service
```

9. Remove the backup files:

```
sudo rm -rf /tmp/patch-3.4.2.1
sudo rm /tmp/fba-patch-3.4.2.1.tar
```

10. Update the Kafka instances to resolve Log4j issues:

```
sudo systemctl status kafka
sudo systemctl stop kafka
sudo systemctl status kafka

sudo rm /usr/lib/kafka/libs/log4j-1.2.17.jar
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-1.2-api-2.18.0.jar
/usr/lib/kafka/libs/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
```

```
/usr/lib/kafka/libs/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/lib/kafka/libs/

sudo chown kafka:kafka /usr/lib/kafka/libs/log4j-1.2-api-2.18.0.jar
sudo chown kafka:kafka /usr/lib/kafka/libs/log4j-core-2.18.0.jar
sudo chown kafka:kafka /usr/lib/kafka/libs/log4j-api-2.18.0.jar
sudo chmod 755 /usr/lib/kafka/libs/log4j-*

sudo rm /usr/lib/zookeeper/lib/log4j-1.2.16.jar
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-1.2-api-2.18.0.jar
/usr/lib/zookeeper/lib/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
/usr/lib/zookeeper/lib/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/lib/zookeeper/lib/

sudo chown zookeeper:zookeeper /usr/lib/zookeeper/lib/log4j-1.2-api-2.18.0.jar
sudo chown zookeeper:zookeeper /usr/lib/zookeeper/lib/log4j-core-2.18.0.jar
sudo chown zookeeper:zookeeper /usr/lib/zookeeper/lib/log4j-api-2.18.0.jar
sudo chmod 644 /usr/lib/zookeeper/lib/log4j-*

sudo rm /usr/lib/zookeeper/contrib/rest/lib/log4j-1.2.15.jar
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-1.2-api-2.18.0.jar
/usr/lib/zookeeper/contrib/rest/lib/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-api-2.18.0.jar
/usr/lib/zookeeper/contrib/rest/lib/
sudo cp /tmp/patch-3.4.2.1/ansible/files/jar/log4j-core-2.18.0.jar
/usr/lib/zookeeper/contrib/rest/lib/

sudo chown zookeeper:zookeeper /usr/lib/zookeeper/contrib/rest/lib/log4j-1.2-api-
2.18.0.jar
sudo chown zookeeper:zookeeper /usr/lib/zookeeper/contrib/rest/lib/log4j-api-
2.18.0.jar
sudo chown zookeeper:zookeeper /usr/lib/zookeeper/contrib/rest/lib/log4j-core-
2.18.0.jar
sudo chmod 644 /usr/lib/zookeeper/contrib/rest/lib/log4j-*
```

11. Restart the Kafka services:

```
sudo systemctl status kafka
sudo systemctl start kafka
sudo systemctl status kafka
```

12. Remove backup files:

```
sudo rm -rf /tmp/patch-3.4.2.1
sudo rm /tmp/fba-patch-3.4.2.1.tar
```

13. Apply new versions of the FBA service `.jar` files. The `.jar` files need to be applied in the following locations:

    MDS/MDSLYTICS:

    <FBA SERVICE HOST>: `mds and mdslytics`

    <FBA SERVICE>: `ro-mds`

    <FBA SERVICE SOURCE FILE> Source file name: `reference-data-service-2.12.2-uberjar.jar`

    <FBA SERVICE DESTINATION FILE> Destination file name:

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

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

14. Copy the Source `<FBA SERVICE>` file to each of the `<FBA SERVICE> HOSTs` in the FBA environment:

```
from the Jenkins host

scp [-i ~/.ssh/my.pem] <SCP_PORT> /data/html/patch-3.4.2.1/ansible/files/jar/<FBA
SERVICE SOURCE FILE> /tmp/<FBA SERVICE DESTINATION FILE>.3.4.2.1

ssh [-i ~/.ssh/my.pem] <SSH_PORT> centos@<FBA SERVICE HOST>-yourenvironment
```

15. Stop the Service:

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

16. Apply the new `.jar` files:

```
cd /usr/lib/java/<FBA SERVICE>
sudo mv /usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar /usr/lib/java/<FBA
SERVICE>/<FBA SERVICE>.jar.pre3.4.2.1
sudo mv /tmp/<FBA SERVICE>.jar.3.4.2.1 /usr/lib/java/<FBA SERVICE>/<FBA
SERVICE>.jar.3.4.2.1
sudo cp -p /usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar.3.4.2.1
/usr/lib/java/<FBA SERVICE>/<FBA SERVICE>.jar
```

17. Start the FBA Service:

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

Important
Steps 14 - 17 must be repeated for each service listed in Step 13.

18. Update the UI with the new version:

```
#from the Jenkins host:
scp [-i ~/.ssh/my.pem] <SCP_PORT> <FBA UI SERVICE> /data/html/patch-
3.4.2.1/ansible/files/rpm/ro-ui-1.101.1-0.7.20221013git3648c2b41a.el7.x86_64.rpm
/tmp/ro-ui-1.101.1-0.7.20221013git3648c2b41a.el7.x86_64.rpm
ssh [-i ~/.ssh/my.pem] <SSH_PORT> centos@<FBA UI SERVICE>-yourenvironment
sudo systemctl stop ro-ui sudo systemctl status ro-ui

#backup the /usr/lib/node_modules/ro-ui folder and contents
sudo tar -cvfz /data/patch-3.4.2.1-backup/ro-ui.backup.tar /usr/lib/node_
modules/ro-ui/

sudo mv /etc/ro-ui/version.yml /etc/ro-ui/version.yml.previous

#install the new UI via the following command:
sudo rpm -Uvh /tmp/ro-ui-1.101.1-0.7.20221013git3648c2b41a.el7.x86_64.rpm
```

19. Restart the service:

```
sudo systemctl start ro-ui
sudo systemctl status ro-ui
```

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

20. Confirm that the patch has been applied and the application is working correctly. Remove backup files from the following locations:

    MDS server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.1`

    MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.1`

    UI server: `/data/patch-3.4.2.1-backup/ro-ui.backup.tar`

INSTALLATION BACKOUT

1. Replace the 3.4.2.1 `.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.pre3.4.2.1`

   MDSlytics server: `/usr/lib/java/ro-mds/ro-mds.jar.pre3.4.2.1`

   # 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>.pre3.4.2.1 /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-3.4.2.1-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
   ```