FIXEdge installation with the principle of least privilege on Linux

Overview

Full access to files is not secure since it can happen that the attacker gets access to highly sensitive information, e.g. from application log files.

It is recommended to set file permissions according to the principle of least privilege.

Since there is no functional necessity for the files containing highly sensitive to be world-readable, the permission should be limited.

This article describes how to specify the privileges satisfying high-security requirements.

Limiting permissions for FIXEdge installation

> **Prerequisites**
>
> It is assumed that FIXEdge was installed according to FIXEdge installation on Linux. Step by step instruction
>
> The guide using /home/user/B2BITS/FIXEdge as FIXEdge installation directory

1. Restrict access to group and other users and remove write permissions for the installation.

```
cd /home/user/B2BITS
chmod -R u-w  FIXEdge/
chmod -R go-rwx  FIXEdge/
```

> Make sure that executable rights for executables are not affected.

2. Enable write permissions for logs directories for FIXEdge and fixicc-agent:

```
chmod -R u+w FIXEdge/FIXEdge1/log/
chmod -R u+w FIXEdge/fixicc-agent/logs/
chmod -R u+w FIXEdge/fixicc-agent/tmp/
```

The minimal access rights configuration required writing access only for FIXEdge logs, fixicc-agent logs and fixicc-agent metadata (FIXEdge/fixicc-agent /tmp/).

Allow configuration changes

In case, when it is required to perform changes in configuration, e.g. to add a new session.

The following commands enable changes in the configuration:

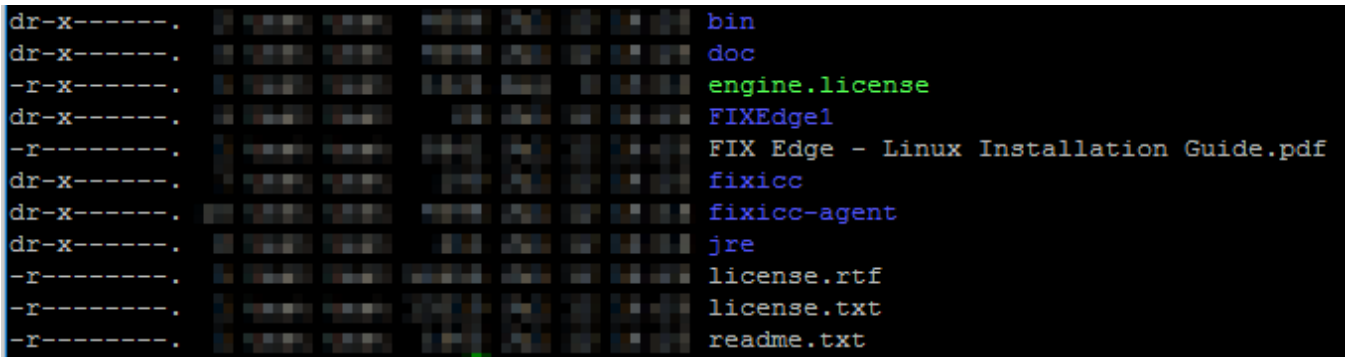
```
chmod -R u+w  FIXEdge/FIXEdge1/conf
chmod -R u+w  FIXEdge/fixicc-agent/conf
```

> The configuration with read-only permissions protects the system from regressions

Check permissions

Make sure that permissions are set only for the current user.

```
ls -l FIXEdge/
```

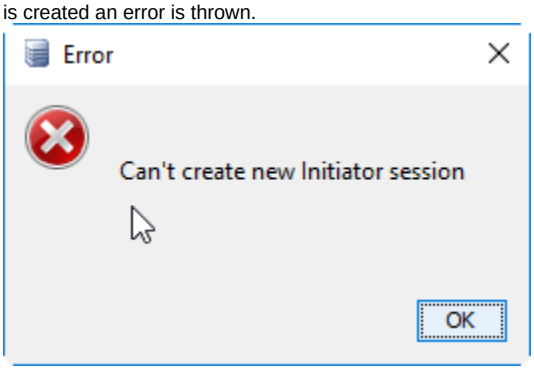


Other notes

- The logs are created with read/write rights for groups and other users.
  But logs directories still have access only for users.

  > the required flags for new logs files can be set via configuring file system ACL attributes or using umask tool

- Super-user privileges are required only once for fixicc-agent installation.
  The rest of the work should be done under a user allowed to run FIXEdge applications.
- It is not recommended to run FIXEdge or fixicc-agent with administrative privileges.
- Creating the backup of the FIXEdge.properties file is not permitted from FIXICC due to access restriction in this case, therefore, after the session is created an error is thrown.



The session is created anyway