



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

SIP Feature Server Deployment Guide

Appendix: Configure JMX port security when running Feature Server with Embedded Cassandra

Appendix: Configure JMX port security when running Feature Server with Embedded Cassandra

Security configuration discussed in this article allows you to protect the JMX management port that is used by the embedded Cassandra module of Feature Servers to communicate with its host process and receive monitoring and management requests. Note that the JMX port is not a data access port.

Embedded Cassandra JMX Authentication

You can follow this procedure to activate the JMX anonymous authentication and view your FS Cassandra nodes status in the FS UI.

Important

This feature is not available for versions prior to 8.1.201.82.

1. Edit the launcher.xml file and set the following parameters to true:
-Dcom.sun.management.jmxremote.authenticate=true
2. Edit the parameter as follows:
-Dcom.sun.management.jmxremote.password.file=./etc/jmxremote.password
3. Copy: jmxremote.password.template
from: /jdk_install_location/jre/lib/management/
to: <FS Installation directory>/etc/
then rename it: jmxremote.password

For OpenJDK 11,
Copy: jmxremote.password.template
from: /jdk_install_location/jre/conf/management/
to: <FS Installation directory>/etc/
then rename it: jmxremote.password
4. Edit the <FS Installation directory>/etc/jmxremote.password file to add the following username:
fsadmin *yourpassword*

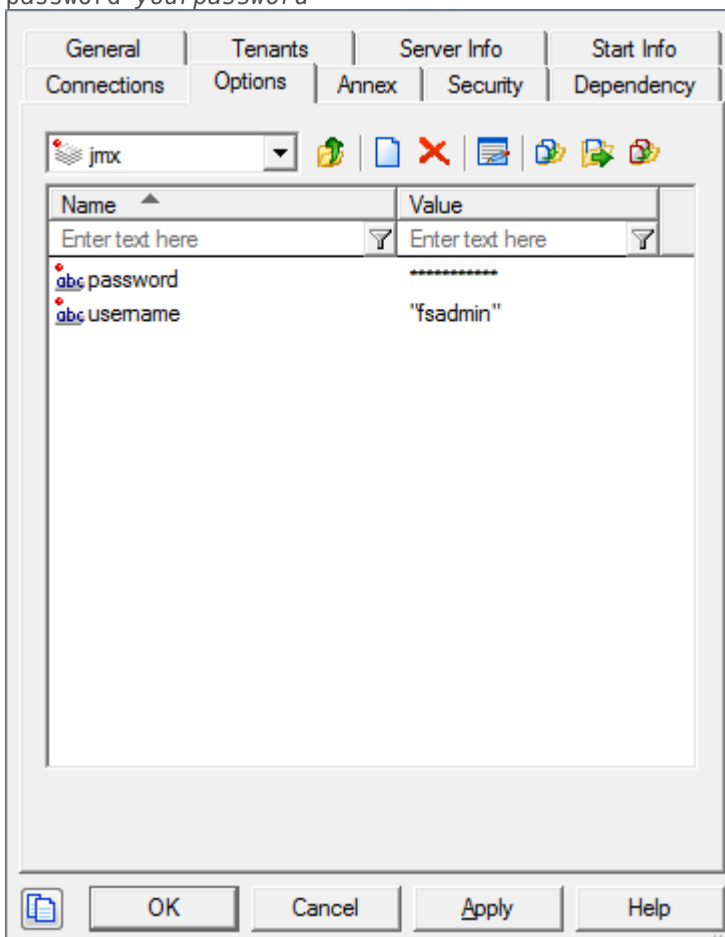
For OpenJDK 11,
Edit the <FS Installation directory>/etc/jmxremote.password file to add the following username:
monitorRole *yourpassword*
controlRole *yourpassword*
fsadmin *yourpassword*
5. Change the ownership of jmxremote.password to the user you run FS with and change permission to read only.

For Linux,

```
chown fsadmin:fsadmin <FS Installation directory>/etc/jmxremote.password
chmod 400 <FS Installation directory>/etc/jmxremote.password
```

For Windows, see the [Oracle documentation](#).

6. Enable read and write permission to the FS user in:
/jdk_install_location/lib/management/jmxremote.access file by adding the following:
fsadmin readwrite
For OpenJDK 11:
Edit /jdk_install_location/conf/management/jmxremote.access file by adding the following:
fsadmin readwrite
7. Edit your FS configuration and create the following options in the **Options** tab:
Section jmx
username=fsadmin
password=*yourpassword*



8. Start FS. You can see the status of the Cassandra nodes by using the Nodetool's ring command. For more details on ring command and its usage, see [Appendix: Performing maintenance operations on embedded Cassandra](#).

Cassandra JMX TLS

A Java Management Extensions (JMX) tool manages and monitors Cassandra. The JMX access must be protected to avoid any remote managing on the FS embedded Cassandra.

1. To protect JMX access, edit the launcher.xml file and modify the parameters as follows:
 - Dcom.sun.management.jmxremote.ssl.enabled.protocols=TLSv1.3
 - Dcom.sun.management.jmxremote.port=9192
 - Dcom.sun.management.jmxremote.ssl=true
 - Dcom.sun.management.jmxremote.authenticate=true
 - Dcom.sun.management.jmxremote.registry.ssl=true
2. Set up Transport Layer Security (TLS). For information on how to create a server certificate, see the [Genesys Security Deployment Guide](#).
3. Create a keystore in <FS Installation directory>/etc/ and upload the custom-generated server certificates to the keystore. See the [Oracle documentation](#).
Note: If FS HTTPS is already enabled with a server certificate, the same keystore and certificate can also be used to secure the embedded Cassandra JMX port.
4. Edit and configure the following JVM options in launcher.xml.
 - javax.net.ssl.trustStore = ./etc/keystore [path of the trust store file]
 - javax.net.ssl.trustStorePassword = <trust store password>
 - javax.net.ssl.keyStore = ./etc/keystore [path of the keystore file]
 - javax.net.ssl.keyStorePassword = <keystore password>
5. Restart the FS to enable a secure JMX connection with the embedded Cassandra.