



FlexMaster

Certificate Renewal Guide

Document Revisions

Version	Date	Description
1.1	March 13, 2017	Initial document

Table of Contents

Document Revisions	2
1. Introduction.....	3
2. Available Scripts	3
3. Applying FM Script on FM	4
4. Applying ZD Script on all ZDs.....	7
5. Changing AP and FM Connection to be HTTP.....	8
5.1. Before FM Certificate Expiration	8
5.2. After FM Certificate Expiration.....	11
6. Appendix: Rolling Back Installed Certificates on FM and ZD.....	14
6.1. Rolling Back the Certificate on FM	14
6.2. Rolling Back the Trusted CA Certificate on ZD.....	16

1. Introduction

The original FlexMaster (a.k.a. FM) certificate will expire on March 26, 2017. Once the certificate expires, the HTTPS connection from Ruckus standalone APs and ZoneDirector (a.k.a. ZD) to FM will not be established any more, as a consequence FM will fail to fetch any data from the AP and the ZD.

To resolve this issue, we recommend customers to upgrade their FM and ZD to version 9.13 or later, and standalone APs to version 104.0 or later. Refer to the FM 9.13.x Release Notes for instructions to upgrade the image.

Customers who do not plan to upgrade their systems, still have the option to follow this guide to renew FM's server certificate, ZD's Trusted CA certificate, and change the standalone AP connection with FM to use HTTP, to avoid this issue.

2. Available Scripts

Three sets of scripts are available to serve:

- **FM Script:** To renew FM server certificate.
- **ZD Script:** To renew ZD Trusted CA certificate.
- **Standalone AP Script:** As one of the options to change AP and FM connection configuration from using HTTPS to HTTP.

NOTE: Customers who need to use HTTPS, must upgrade their standalone AP and FM to newer versions (ap_104.0 and FM_9.13.x or later).

Use the following tables to learn which script(s) should be applied in your system:

Table 1. ZDs managed by FM

	ZD 9.9/9.10.0/9.10.1/9.12.0/9.12.1 or earlier version	ZD_9.10.2/9.12.2/9.12.3	ZD 9.13.X or later version
FM 9.9/9.10.0/9.10.1/9.12.0 /9.12.1 or earlier version	Apply both FM and ZD Scripts	Not applicable ¹	
FM 9.10.2 or FM 9.12.2	Apply both FM and ZD Scripts	Apply FM Script	Not applicable ¹
FM 9.13.x or later version	Apply ZD Script	Certificates are new on ZD and FM already, no action is needed.	

Table 2. Standalone APs managed by FM

AP 9.8.x or earlier version	AP_100.0	AP_100.1	AP_100.2	AP_104.0
Use either FM Web UI, AP WebUI/CLI, or Standalone AP Script to change AP-FM connection from HTTPS to HTTP				AP certificates are new already. FM must be upgraded to FM_9.13.x or later, or use either FM Web UI, AP WebUI/CLI, or Standalone AP Script to change AP-FM connection from HTTPS to HTTP

¹ FM doesn't officially support ZD running higher versions than FM version.

3. Applying FM Script on FM

File name: **fmNewCert.tar**

MD5: 8B5ED9019AF9B0DA5FC04030DBE6112B

Following is an example:

a) Upload FM script to the FM server and copy it to the FM folder (by default it is /opt/FM)

b) Extract ("un-tar") FM script:

```
[root@localhost FM]# cd /opt/FM/
[root@localhost FM]# tar -vxf fmNewCert.tar
upgradeKeystore.sh
.keystore.20160201
```

c) Apply FM Script:

```
[root@wifiFM FM]# pwd
/opt/FM
[root@wifiFM FM]# ./upgradeKeystore.sh
/opt/FM
```

Restarting FM...

```
shutdown_pid=14819
Shutting down Tomcat server...
```

```
Using CATALINA_BASE: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42
Using CATALINA_HOME: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42
Using CATALINA_TMPDIR: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/temp
Using JRE_HOME: /opt/FM/3rdparty/jre/jre1.6.0_45
Using CLASSPATH: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/bootstrap.jar:/opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/tomcat-juli.jar
Going to kill FM process.
Done.
Going to kill FM process.
killing HttpShellProxy process pid=13026
Done.
Going to kill Snmpagent process.
killing Snmpagent process pid=13050
Done.
Warning: Using a password on the command line interface can be insecure.
Current path = /opt/FM/support_files
waiting...test -e /opt/FM/3rdparty/mysql/mysql-advanced-5.6.13-linux-glibc2.5-x86_64/data/wifiFM.pid
file check=not
```

Linux version [x86_64]

```
JAVA_OPTS=-server -Xms2187m -Xmn1914m -Xmx5104m -XX:PermSize=256m -  
XX:MaxPermSize=256m -XX:+HeapDumpOnOutOfMemoryError -XX:-  
UseGCOverheadLimit -Djava.awt.headless=true -Xss2m  
startup_pid=14941  
Starting MySQL server.
```

```
170217 07:41:40 mysqld_safe Logging to '/opt/FM/3rdparty/mysql/mysql-advanced-  
5.6.13-linux-glibc2.5-x86_64/data/wifiFM.err'.  
170217 07:41:40 mysqld_safe Starting mysqld daemon with databases from  
/opt/FM/3rdparty/mysql/mysql-advanced-5.6.13-linux-glibc2.5-x86_64/data  
Detecting MySQL status...  
MySQL start successfully!  
Starting ActiveMQ.
```

```
nohup: appending output to `nohup.out'  
Starting Tomcat server.
```

```
Using CATALINA_BASE: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42  
Using CATALINA_HOME: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42  
Using CATALINA_TMPDIR: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/temp  
Using JRE_HOME: /opt/FM/3rdparty/jre/jre1.6.0_45  
Using CLASSPATH: /opt/FM/3rdparty/tomcat/apache-tomcat-  
7.0.42/bin/bootstrap.jar:/opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/tomcat-  
juli.jar  
Using CATALINA_BASE: /opt/FM/3rdparty/tomcat/httpshellproxy  
Using CATALINA_HOME: /opt/FM/3rdparty/tomcat/httpshellproxy  
Using CATALINA_TMPDIR: /opt/FM/3rdparty/tomcat/httpshellproxy/temp  
Using JRE_HOME: /opt/FM/3rdparty/jre/jre1.6.0_45  
Starting snmpagent at port 161.
```

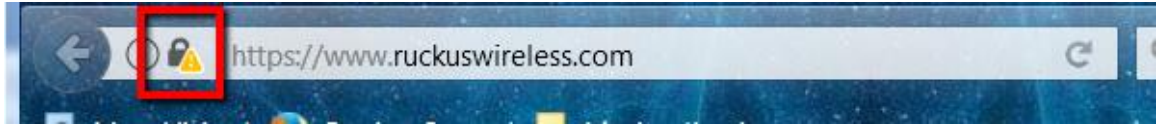
SNMP agent starts up successfully.

```
[root@wifiFM FM]#
```

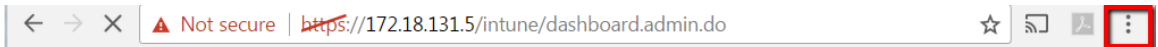
d) [Verify FM certificate status](#)

Open a web browser and login to FM via HTTPS, and verify the validity period of the certificates; it should be valid through Aug 1st (or Aug 2nd, depending on your time zone), 2040.

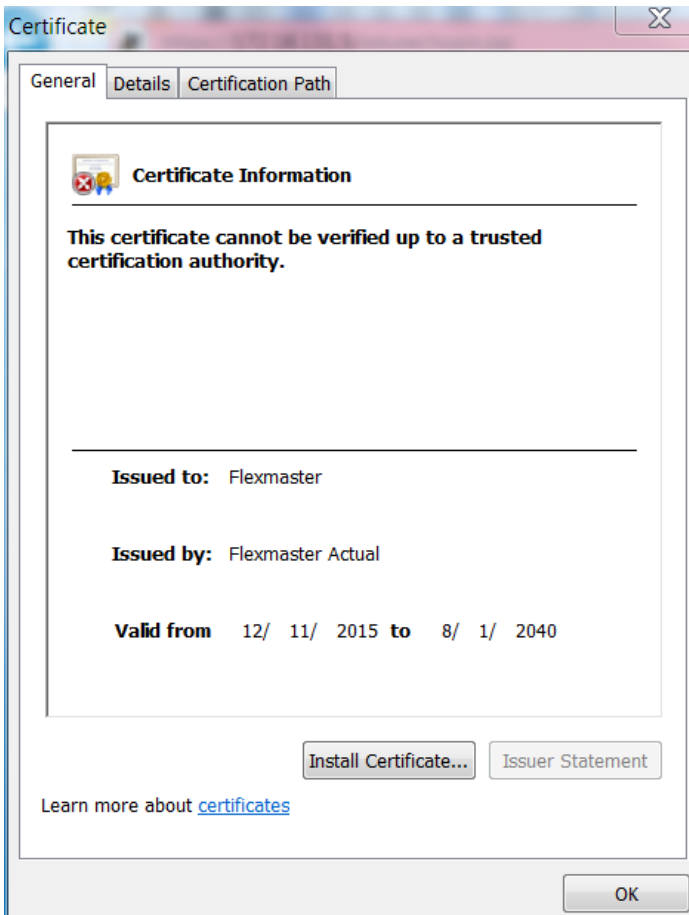
For example, on a Firefox browser, click the browser's **certificate icon** as follows, and then navigate to **Security** tab and then click **View Certificate** to confirm the expiration date.



On a Chrome browser, click the **Customerize and control Google Chrome icon** as shown below, and select **More Tools**. Then select **Developer tools**. Show the **Security** tab (you may need to click the >> icon to have the tab shown). And then select **View certificate** to verify the expiration date of the certificate.



On an Internet Explorer browser or a Safari browser, click the **certificate icon** at the end of the URL bar to confirm:



4. Applying ZD Script on all ZDs

File name: import-fmcacert_v10.tar.gz

MD5 checksum value (can be used to verify file integrity):

38BDE94A7F6AC472DF51F3A4CD22E76E

Following is an example:

- a) Import ZD script into ZD through ZD Web UI from Administrator->Diagnostics->Import scripts.
- b) Establish a SSH session to ZD CLI. Execute imported script:

```
ruckus> enable
```

```
ruckus# debug
```

You have all rights in this mode.

```
ruckus(debug)# script
```

```
ruckus(script)# list
```

Index	Scripts
1	import-fmcacert.sh

```
ruckus(script)# exec import-fmcacert.sh
```

Import new FM CA successfully.

Restart tr069d.

```
ruckus(script)#
```

Note 1: If the ZD device is ZD1100, it may display the following warning when the script is applied. This is an expected result, and you can ignore it.

```
ruckus(script)# exec import-fmcacert.sh
```

```
sed: /file_list.txt: No such file or directory
```

Import new FM CA successfully.

Restart tr069d.

Note 2: Once the FM CA certificate is imported, it will be preserved even if ZD is rebooted or set to factory default. But if ZD is upgraded to a version that doesn't have a new CA certificate, this script must be executed again. ZD 9.10.2/9.12.2/9.12.3/9.13 and later versions have the new FM CA certificate.

5. Changing AP and FM Connection to be HTTP

We recommend that customers upgrade their Standalone AP and FM to the latest version (104.0 and 9.13.x or later) to avoid the FM certificate expiration issue after March 26, 2017.

However, for customers who do not plan to upgrade their Standalone APs, you can change the FM server URL to HTTP to bypass the issue.

Note: Customers who need to use HTTPS, must upgrade their Standalone AP to version 104.0 and FM to version 9.13.x or later.

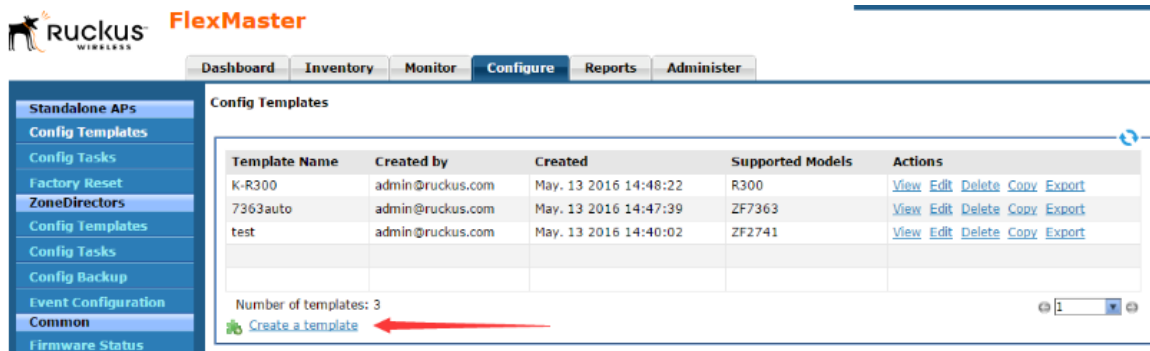
5.1. Before FM Certificate Expiration

If the FM certificate has not expired, and if the standalone AP can still connect to FM, you can follow the example to change FM server URL to HTTP through the FM template or FM Web UI.

Option 1: Use FM template:

Steps:

1. Login to FM using the root account
2. Go to Configure -> Standalone APs -> Config Templates
3. Click **Create a template**



The screenshot shows the Ruckus FlexMaster web interface. The navigation menu on the left includes: Standalone APs, Config Templates, Config Tasks, Factory Reset, ZoneDirectors, Config Templates, Config Tasks, Config Backup, Event Configuration, Common, and Firmware Status. The main content area is titled 'Config Templates' and contains a table with the following data:

Template Name	Created by	Created	Supported Models	Actions
K-R300	admin@ruckus.com	May. 13 2016 14:48:22	R300	View Edit Delete Copy Export
7363auto	admin@ruckus.com	May. 13 2016 14:47:39	ZF7363	View Edit Delete Copy Export
test	admin@ruckus.com	May. 13 2016 14:40:02	ZF2741	View Edit Delete Copy Export

Below the table, it says 'Number of templates: 3' and there is a 'Create a template' link with a green plus icon. A red arrow points to this link.

4. Type a name, and choose "Management Server Configuration Setting"

CREATE A TEMPLATE

Template Name: FM URL

Product Type: ZF2741

Select product type: Ruckus ZF2741 Device

Select the configuration options that you want to modify:

- Select All
- Device Group
- Internet
- Local Subnet
- Local Subnet
- Local Subnet
- Local Subnet
- Wireless
- Wireless
- Wireless
- Wireless
- Wireless 4
- Wireless 5
- Management Server Configuration Settings

5. Check "Device Registration Settings" then click **Next**

Template Name: FM URL

Product Type: ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962,ZF7762,ZF7731,ZF7341,ZF7343,ZF7363,ZF7025,ZF7321,ZF7982,ZF7762-T,ZF7762-AC,ZF7762-S-AC,ZF7761CM,ZF7341,ZF7782,ZF7782-S,ZF7782-N,ZF7782-E,ZF7372,ZF7352,SC8800-S,SC8800-S-AC,ZF7321-U,ZF7055,ZF7781FN,ZF7781FN-E,ZF7781FN-S,ZF7781CM,ZF7781CM-E,ZF7781CM-S,ZF7351,ZF7372-E,ZF7441,R300,R700,R500,T300,T301N,R600,T301S,T300E,H500,P300,R710,R310,T710,T710S,R510

Select product type: Management Server Configuration Settings

Select the configuration options that you want to modify:

- Select All
- Device Registration Settings

Back Next

6. In parameter detail page, choose "Server URL" and configure it to use HTTP. Note the full URL needs to be used.

Device Registration Settings

Parameter	Value
<input checked="" type="checkbox"/> Server URL:	http://172.18.131.2/intune/server
<input type="checkbox"/> Server Registration User Name:	
<input type="checkbox"/> Server Registration Password:	
<input type="checkbox"/> Periodic Inform Interval:	15 Minutes
<input type="checkbox"/> Remote Management Mode:	FlexMaster

Warning: If this value is incorrect, the device will not be able to contact the FlexMaster server.

Warning: Once SNMP is enabled, the CPE will no longer be managed by FlexMaster.

Back Next Cancel

7. Click **Next** and then **Save**

Configuration Parameters and Values

Persist selected settings after a factory reset

Parameter Name	Parameter Value	Validation
Server URL:	http://172.18.131.2/intune/server	

Back Save Cancel

8. Go to Standalone APs -> Config Tasks -> Create a task to configure the APs. Select appropriate devices.

Dashboard Inventory Monitor **Configure** Re

Standalone APs

- Config Templates
- Config Tasks**
- Factory Reset
- ZoneDirectors
- Config Templates
- Config Tasks
- Config Backup
- Event Configuration
- Common
- Firmware Status
- Firmware Upgrade

Config Tasks

ID	Task Name	Schedule

Number of tasks: 0

[Create a task](#)

CREATE A TASK

Task Settings

Specify a task name:

Select a configuration template:
 FM URL (ZF2925,ZF2942,VF2825,VF7811,ZF7942,VF2811,ZF2741,ZF7962,ZF7762,ZF7731,ZF7341,ZF7343,ZF7363,ZF7025,ZF7321,ZF798
[View Parameters](#)

Select the devices to be provisioned

Select View **Select Devices** Advanced Settings

Select a view of devices to perform configuration update: All Standalone APs [View Details](#)

Device Name	Serial #	MAC Address	IP Address	External IP Address	Model	Connection	Uptime	Software	Tag
RuckusAP	301003000244	AC:67:06:1E:45:30	192.168.0.100:443	172.18.131.8:443	ZF7962	✓	200d 3h 34m	9.6.0.0.47	

Option 2: Use FM AP Device View

Steps:

1. Login to FM and go to Inventory --> Standalone, click the Serial Number of the Standalone AP to pop up the Standalone AP Device View.
2. Go to Standalone AP Device View --> Detail → Device, click **Edit Setting** and change the Server URL to use HTTP.



FlexMaster

Summary Details Diagnostics

Device

Device Name: 7982

Periodic Inform Interval: 1 minute

Server URL: http://172.18.56.14/intune/server

Service Provider Login Name: super

Service Provider Login Password:

Service Provider Password Confirmation:

LED Control: Disable Status LED(s)

TACACS+ State:

Back Submit Reset

5.2. After FM Certificate Expiration

If the FM certificate has expired and the Standalone AP is disconnect from FM, we recommend that customers use Standalone AP Web UI, AP CLI, or Standalone AP Script to change the FM server URL to HTTP.

Option 1: Change on Standalone AP Web UI

Login to the Standalone AP Web UI and change FM server URL to use HTTP:

Device

Internet

Local Subnets

Radio 2.4G

Radio 5G

Ethernet Ports

Hotspot

Maintenance

Upgrade

Reboot / Reset

Support Info

Administration

Management

Diagnostics

Log

TR069 / SNMP Management Choice

Auto (SNMP and TR069 will work together.)

SNMP only

FlexMaster only

None

DHCP Discovery: https://flexmaster/intune/server

FlexMaster Server URL: http://172.18.56.14/intune/server

Digest-authentication Username: 712b4265b294772f31344f2e6

Digest-authentication Password: 10663476AAC793836579BD8

Periodic FlexMaster Inform Interval: 1 minute

TR069 Status

Currently Using URL: https://172.18.56.14/intune/server

Last Attempted Contact: 2016-07-18 03:31:12 GMT using https://172.18.56.14/intune/server

Last Successful Contact: 2016-07-18 03:31:12 GMT using https://172.18.56.14/intune/server

Last Contact Result: Successful

Current Time: Mon Jul 18 03:32:00 2016 (UTC)

Option 2: Change on Standalone AP CLI:

Use the following command (SSH (or Telnet) to Standalone AP CLI) and change the TR069 URL to HTTP:

```
rksccli: set tr069 url http://10.11.158.8/intune/server
```

Option 3: Apply Standalone AP Script on FM:

File name: **changeTr069Protocol.sh**

MD5: AC3BD3009B857946B11B6501A868C1DC

File name: **SwitchAPTr069Protocol.sh**

MD5: 380D0C03899BDCE1A1EF99A9CA682B80

Caveats and Limitations on Standalone AP Script:

Before following the script to apply AP Script, be aware of the following:

- If APs are located within a NAT/Firewall, the scripts may not be able to reach them from the FM server to make it work.
- This script depends on the script tool '**expect**' package. Before running the script make sure 'expect' is installed on the system. To install 'expect' you can execute the command 'yum install expect'.
- In case the FM is freshly installed, or Standalone AP View is newly created, wait for 20 minutes to make sure the system completely synchronizes with the DataBase, and then execute the script.

Steps:

1. Download the two Standalone AP script files on the FM server.
2. Copy the script files to \$FM_HOME/support_files/ and make them executable (chmod to 770).

For example, if FM is installed in /opt/FM/, copy the script files in /opt/FM/support_files/

```
[root@localhost support_files]# chmod 770 SwitchAPTr069Protocol.sh  
[root@localhost support_files]# chmod 770 changeTr069Protocol.sh
```

3. Change the directory to \$FM_HOME/support_files/,

issue command: /SwitchAPTr069Protocol.sh \$FM_HOME '\$mysql_username'
'\$mysql_password';

select view_id which will be after this step and input the new HTTP TR069 url to run the scripts.

For example: ./SwitchAPTr069Protocol.sh /opt/FM 'root' 'admin!234'

```

[root@localhost FlexMaster]# cd support_files/
[root@localhost support_files]# pwd
/FlexMaster/support_files
[root@localhost support_files]# ./SwitchAPTr069Protocol.sh /FlexMaster 'root' 'admin!234'
fetch all SOLO AP views
Warning: Using a password on the command line interface can be insecure.
view id, view name
1, All Standalone APs
4, Bali
Please enter the view_id.
view id:4
Please enter the intune server url.
url:http://10.11.158.8/intune/server
fetch the devices in the view: 4
Warning: Using a password on the command line interface can be insecure.
1, RuckusWB, 10.11.158.26, 74:91:1A:10:DB:00, super, sp-admin
spawn ssh -l super 10.11.158.26

Please login: super
password :
Copyright (C) 2005-2010 Ruckus Wireless, Inc. All Rights Reserved.
rksccli: set tr069 url http://10.11.158.8/intune/server
OK
2, RuckusWB, 10.11.158.27, 74:91:1A:10:DA:F0, kenneth, admin!234
spawn ssh -l kenneth 10.11.158.27

Please login: kenneth
password :
Copyright (C) 2005-2010 Ruckus Wireless, Inc. All Rights Reserved.
rksccli: set tr069 url http://10.11.158.8/intune/server
OK
[root@localhost support_files]#

```

4. Check the logs (Success/Failed) in \$FM_HOME/switchSoloAP/

```

[root@localhost support_files]# cd ..
[root@localhost FlexMaster]# ls
3rdparty  conf          fmscript.log  README.txt  restore.sh  snmpagent.log  support_files  uninstall.sh  webapps
backup.sh  fm_db_rep.sh  install.log   restart.sh  shutdown.sh  startup.sh     switchSoloAP  upgrade.sh    zdbackup
[root@localhost switchSoloAP]# ls
failed_20170228142538.log  success_20170228142538.log
[root@localhost switchSoloAP]# cat failed_20170228142538.log
device name, IP, MAC, error
[root@localhost switchSoloAP]# cat success_20170228142538.log
device name, IP, MAC
RuckusWB, 10.11.158.26, 74:91:1A:10:DB:00
RuckusWB, 10.11.158.27, 74:91:1A:10:DA:F0
[root@localhost switchSoloAP]#

```

6. Appendix: Rolling Back Installed Certificates on FM and ZD

In a rare case that the user needs to roll back installed certificates, this section provides the instructions.

Warning: after executing the following instructions the system will be with the old certificates that expires on March 26, 2017.

6.1. Rolling Back the Certificate on FM

While applying the renewed FM certificate script, the original script is automatically backed-up.:

Backup folder: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.25/conf/

Backup File name: .keystore.2006.{timestamp}.bak

```
[root@localhost FM]# cd /opt/FM/
```

```
[root@wifiFM FM]# cd /3rdparty/tomcat/apache-tomcat-7.0.42/conf/
```

```
[root@wifiFM conf]# ls -ltra
```

```
total 232
```

```
-rw-----. 1 root root 162905 Jul 2 2013 web.xml
```

```
-rw-----. 1 root root 5946 Jul 2 2013 catalina.properties
```

```
-rw-----. 1 root root 11893 Jul 2 2013 catalina.policy
```

```
drwxr-xr-x. 9 root root 4096 Feb 17 13:56 ..
```

```
-rw-----. 1 root root 6435 Feb 17 13:56 server.xml.org
```

```
-rw-----. 1 root root 2876 Feb 17 13:56 logging.properties
```

```
-rw-----. 1 root root 1394 Feb 17 13:56 context.xml
```

```
-rw-----. 1 root root 197 Feb 17 13:56 tomcat-users.xml
```

```
drwxr-xr-x. 3 root root 4096 Feb 17 14:00 Catalina
```

```
-rw-----. 1 root root 6840 Feb 17 14:31 server.xml
```

```
-r--r--r--. 1 root root 2413 Feb 17 15:41 .keystore.20160201
```

```
drwxr-xr-x. 3 root root 4096 Feb 17 15:41 .
```

```
-r--r--r--. 1 root root 4029 Feb 17 15:41 .keystore.2006.20170217154131.bak
```

```
-r--r--r--. 1 root root 2413 Feb 17 15:41 .keystore
```

```
[root@wifiFM conf]# pwd
```

```
/opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/conf
```

```
[root@wifiFM conf]# cp .keystore.2006.20170217154131.bak .keystore
```

```
cp: overwrite `'.keystore'? y
```

```
[root@wifiFM conf]# cd /opt/FM/
```

```
[root@wifiFM FM]# ./restart.sh
```

Restarting FM...

shutdown_pid=16308

Shutting down Tomcat server...

Using CATALINA_BASE: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42

Using CATALINA_HOME: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42

Using CATALINA_TMPDIR: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/temp

Using JRE_HOME: /opt/FM/3rdparty/jre/jre1.6.0_45

Using CLASSPATH: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/bootstrap.jar:/opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/tomcat-juli.jar

Going to kill FM process.

Done.

Going to kill FM process.

killing HttpShellProxy process pid=15711

Done.

Going to kill Snmpagent process.

killing Snmpagent process pid=15738

Done.

Warning: Using a password on the command line interface can be insecure.

170217 07:52:10 mysqld_safe mysqld from pid file /opt/FM/3rdparty/mysql/mysql-advanced-5.6.13-linux-glibc2.5-x86_64/data/wifiFM.pid ended

Current path = /opt/FM/support_files

waiting...test -e /opt/FM/3rdparty/mysql/mysql-advanced-5.6.13-linux-glibc2.5-x86_64/data/wifiFM.pid

file check=not

Linux version [x86_64]

JAVA_OPTS=-server -Xms2187m -Xmn1914m -Xmx5105m -XX:PermSize=256m -XX:MaxPermSize=256m -XX:+HeapDumpOnOutOfMemoryError -XX:-UseGCOverheadLimit -Djava.awt.headless=true -Xss2m

startup_pid=16434

Starting MySQL server.

```
170217 07:52:13 mysqld_safe Logging to '/opt/FM/3rdparty/mysql/mysql-advanced-5.6.13-linux-glibc2.5-x86_64/data/wifiFM.err'.
```

```
170217 07:52:13 mysqld_safe Starting mysqld daemon with databases from /opt/FM/3rdparty/mysql/mysql-advanced-5.6.13-linux-glibc2.5-x86_64/data
```

```
Detecting MySQL status...
```

```
MySQL start successfully!
```

```
Starting ActiveMQ.
```

```
nohup: appending output to `nohup.out'
```

```
Starting Tomcat server.
```

```
Using CATALINA_BASE: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42
```

```
Using CATALINA_HOME: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42
```

```
Using CATALINA_TMPDIR: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/temp
```

```
Using JRE_HOME: /opt/FM/3rdparty/jre/jre1.6.0_45
```

```
Using CLASSPATH: /opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/bootstrap.jar:/opt/FM/3rdparty/tomcat/apache-tomcat-7.0.42/bin/tomcat-juli.jar
```

```
Using CATALINA_BASE: /opt/FM/3rdparty/tomcat/httpshellproxy
```

```
Using CATALINA_HOME: /opt/FM/3rdparty/tomcat/httpshellproxy
```

```
Using CATALINA_TMPDIR: /opt/FM/3rdparty/tomcat/httpshellproxy/temp
```

```
Using JRE_HOME: /opt/FM/3rdparty/jre/jre1.6.0_45
```

```
Starting snmpagent at port 161.
```

```
SNMP agent starts up successfully.
```

```
[root@wifiFM FM]#
```

6.2. Rolling Back the Trusted CA Certificate on ZD

When you execute the script to upgrade the CA cert, the original CA certificate is automatically backed-up. To roll back to the original CA cert, execute the same script on ZD CLI as follows:

```
ruckus> enable
```

```
ruckus# debug
```

```
You have all rights in this mode.
```

```
ruckus(debug)# script
```

```
ruckus(script)# list
```


Index	Scripts
1	import-fmcacert.sh

```
ruckus(script)# exec import-fmcacert.sh recovery  
Recover successfully.  
Restart tr069d.  
ruckus(script)#
```

[End of Document]