User Guide RFSToolv4 2.10

System Module Recovery with Restore Factory Settings

Radio Network
AirScale BTS LTE
AirScale BTS TD-LTE
Flexi Multiradio BTS WCDMA
Flexi Multiradio BTS LTE
Flexi Multiradio BTS TD-LTE
Flexi Multiradio 10 BTS EDGE
Flexi Multiradio BTS EDGE
Single RAN
Flexi Lite BTS WCDMA
Flexi Zone WCDMA BTS
Flexi Zone BTS TD-LTE
Flexi Zone BTS

Approval date: (08-Dec-2017)

This document contains following type of information	
Informative	
Preventive	X
Corrective	
Additional categorization	
Urgent	X
Security	
Release Upgrade	
SW Update	
Parameterization	
Information is classified as	
Internal	
Public	X
Customer Specific	

Table of Contents

Contact:

Contact your local Nokia support

Summary of changes:

Date	Version	Change Description
13-May-2017	0.1	Draft for RFSToolv4 2.03
04-Aug-2017	1.0	Approved for RFSToolv4 2.04
16-Aug-2017	1.1	Updated for RFSToolv4 2.05
23-Aug-2017	2.0	Approved for RFSToolv4 2.07
23-Oct-2017	2.1	Updated for RFSToolv4 2.08
07-Nov-2017	2.2	Updated for RFSToolv4 2.09
08-Nov-2017	2.3	Updated for RFSToolv4 2.10
08-Dec-2017	2.4	Updated for RFSToolv4 2.10

Content in issue 0.1

RFSToolv4 application 2.03 (12 May 2017)

- RFSToolv3 1.50 used as a baseline.
- ASIA support added – FL17 & FL17SP support added.
- WBTSZ17 support added for Flexi Zone WCDMA BTS.
- FSMFA support added.
- Added FZM scenario to identify permanent code load - flash failure.
- 7.4.1 Password encryption command has changed. (‘-pwd’ => ‘-W’)

Changes between issues 0.1 and 1.0

RFSToolv4 application 2.04 (04 Aug 2017)

- Chapter 3.1. Updated SW compatibility table.
  - FSMF, ASIA support updated – xL17 & xL17SP support added.
  - FDSW information added.
- Merged RFSToolv3 1.51-1.59 content to RFSToolv4 2.04.

  RFSToolv3 application **1.51** (10 May 2017)
  - Corrected WCDMA license file removal scenario.
  - Corrected WCDMA FSME recovery scenario, sometimes file flashing was halted due to password issue.
  - NOLS release. TS-SRAN-HW-0080-I7.

  RFSToolv3 application **1.56** (04 Jul 2017)
  - Added Operator certificate removal scenario for FSME.
  - Added correction to failed password reset/SW update during sanity check + SW update scenario.

  RFSToolv3 application **1.58** (02 Aug 2017)
  - FSME/FSMD: Improved SW update scenario in FL16A, unnecessary TCP connections were left open while SW update was started. It made recovery scenario systematically to fail with FL16A 7.0. Correction will impact WCDMA scenarios as well.

  RFSToolv3 application **1.59** (03 Aug 2017)
  - FSME/FSMD: Corrected SSH connectivity and password management connected to operator certificate removal.

RFSToolv4 2.04 will replace RFSToolv3 (all versions).

Changes between issues 1.0 and 1.1

RFSToolv4 application 2.05 (16 Aug 2017)

- Corrected encrypted password file handling problem when using password file is equipped with one login-password entry. Option 4 was causing the following SW update to fail.

Changes between issues 1.1 and 2.0

RFSToolv4 application 2.07 (23 Aug 2017)

- Corrected operator certificate and BTS configuration removal scenario (item 4 in Remove Operator Certificate). It caused the following SW update with FSMF to fail.
- Corrected temporary folder handling & cleanup used during SW update.
- Released for BTS Site manager delivery.

WBTSZ17	WL9.1_BTSSM_1408_104_00
FL17	FL17_BTSSM_0000_000307_000000
FL17SP	FL17SP_BTSSM_0000_000364_000000
FL17A	FL17A_BTSSM_0000_000327_000000
TL17	TL17_BTSSM_0000_000285_000000
TL17SP	TL17SP_BTSSM_0000_000316_000000
TL17A	TL17A_BTSSM_0000_000309_000000
WBTS18	WBTS18_BTSSM_0_199_0
WBTS17	WBTS17_BTSSM_1606_155_00
FLC17A	FLC17A_BTSSM_0000_000151_000000
TLC17A	TLC17A_BTSSM_0000_000144_000000
FLF17SP	FLF17SP_BTSSM_0000_000208_000000
FLF17A	FLF17A_BTSSM_1708_000212_000000
TLF17SP	TLF17SP_BTSSM_0000_000199_000000
TLF17A	TLF17A_BTSSM_0000_000208_000000

Changes between issues 2.0 and 2.1

RFSToolv4 application 2.08 (23 Oct 2017)

- Corrected operator certificate and BTS configuration removal scenario (item 4 in Remove Operator Certificate). It caused the following SW update with FSMF to fail.
- Added support for ASIAA 474403A.

Changes between issues 2.1 and 2.2

RFSToolv4 application 2.09 (07 Nov 2017)

- The need of additional reset removed when FSMF is upgraded to loads such as LN7.0. Previously additional reset was required to gain access to FSMF with 2G BTS Site manager or e.g. LTE BTS Site manager. In practice FSMF is power cycled.
- Service account credentials are updated to default ones during GF to other RAT update.
- Corrected issue for FSMF when upgrading from SRAN17A to FL17A and ‘clear BTS configuration’ is not selected – this caused restore routine to fail.
- Corrected issue for FSMF where some of the SRAN specific files were not signed during SW update.

Changes between issues 2.2 and 2.3

RFSToolv4 application 2.10 (08 Nov 2017)

- Removed swconfig.txt usage during restore procedure. SRAN17A support released

Changes between issues 2.3 and 2.4

RFSToolv4 application 2.10 (08 Nov 2017)

- NOLS release. TS-SRAN-HW-0080-I8. Documentation update.

Last restore tool version is equipped to carry all items listed in the change history.

Disclaimer

The information in this document applies solely to the hardware/software product (“Product”) specified herein, and only as specified herein. Reference to “Nokia” later in this document shall mean the respective company within Nokia Group of Companies with whom you have entered into the Agreement (as defined below).

This document is intended for use by Nokia's customers (“You”) only, and it may not be used except for the purposes defined in the agreement between You and Nokia (“Agreement”) under which this document is distributed. No part of this document may be used, copied, reproduced, modified or transmitted in any form or means without the prior written permission of Nokia. If You have not entered into an Agreement applicable to the Product, or if that Agreement has expired or has been terminated, You may not use this document in any manner and You are obliged to return it to Nokia and destroy or delete any copies thereof.

The document has been prepared to be used by professional and properly trained personnel, and You assume full responsibility when using it. Nokia welcomes your comments as part of the process of continuous development and improvement of the documentation.

This document and its contents are provided as a convenience to You. Any information or statements concerning the suitability, capacity, fitness for purpose or performance of the Product are given solely on an “as is” and “as available” basis in this document, and Nokia reserves the right to change any such information and statements without notice. Nokia has made all reasonable efforts to ensure that the content of this document is adequate and free of material errors and omissions, and Nokia will correct errors that You identify in this document. Nokia's total liability for any errors in the document is strictly limited to the correction of such error(s). Nokia does not warrant that the use of the software in the Product will be uninterrupted or error-free.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

This tool, files and all associated documentation (“Tool”) is privileged, confidential and protected under law.

Downloading, using or accessing this Tool requires a written license agreement from Nokia. Any unauthorized use, access or distribution is illegal and strictly prohibited without a written license from Nokia

Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

⚠ Important Notice on Product Safety

This product may present safety risks due to laser, electricity, heat, and other sources of danger.

Only trained and qualified personnel may install, operate, maintain or otherwise handle this product and only after having carefully read the safety information applicable to this product.

The safety information is provided in the Safety Information section in the “Legal, Safety and Environmental Information” part of this document or documentation set.

Nokia is continually striving to reduce the adverse environmental effects of its products and services. We would like to encourage you as our customers and users to join us in working towards a cleaner, safer environment. Please recycle product packaging and follow the recommendations for power use and proper disposal of our products and their components.

If you should have questions regarding our Environmental Policy or any of the environmental services we offer, please contact us at Nokia for any additional information.

1. PURPOSE

This document contains generic information about products. These can be instructions that explain problem situations in the field, instructions on how to prevent or how to recover from problem situations, announcements about changes or preliminary information as requirements for new features or releases.

2. VALIDITY

2.1 Impacted technology

Technology	Impact
GSM/EDGE	X
WCDMA	X
LTE-FDD	X
LTE-TD	X
SRAN	X

2.2 Impacted system and software releases

System Release	Product SW Release(s)
AirScale BTS LTE	FL16A, FL17A
AirScale BTS TD-LTE	TL16A, TL17A
Flexi Multiradio LTE BTS	FL16, FL16A, FL17A
Flexi Multiradio TD-LTE BTS	TL16, TL16A, TL17A
Flexi Multiradio WCDMA BTS	WN9.1, WBTS16, WBTS17, WBTS18
Single RAN	S16.10, SBTS17A
Flexi Multiradio 10 BTS EDGE	GF16, GF17
Flexi Lite BTS WCDMA	WL7.0 2.0, WL8.0, WL9.1
Flexi Zone WCDMA BTS	WZ9.1, WBTSZ17
Flexi Zone BTS TD-LTE	TLF16A, TLF17A
Flexi Zone BTS	FLF17A, FLC16A, FLC17A
System Module Factory Delivery SW	FDSW1.3, FDSW1.4, FDSW2.0, FDSW2.1

2.3 Impacted products

Product	Product Code
AirScale System Module, ASIA	473095A
AirScale System Module, ASIAA	474403A
Flexi Multiradio 10 System Module, FSMF	472181A
Flexi Multiradio 10 System Module, FSMFA	473585A
Flexi Multiradio 10 System Module, FSIH	472567A
Flexi Multiradio System Module, FSME	471469A
Flexi Multiradio System Module, FSMD	471402A
Flexi Multiradio System Module, FSMC	471401A
Flexi Lite BTS WCDMA, FQGA	472467A
Flexi Lite BTS WCDMA, FQFA	472751A
Flexi Zone WCDMA BTS, FWGL	473233A
Flexi Zone WCDMA BTS, FWGM	473234A
Flexi Zone WCDMA BTS, FWGN	473235A
Flexi Zone WCDMA BTS, FWFE	473236A
Flexi Zone WCDMA BTS, FWFF	473237A
Flexi Zone WCDMA BTS, FWFG	473238A
Flexi Zone WCDMA BTS, FWFI	473771A
Flexi Zone WCDMA BTS, FWGP	473993A
Flexi Zone BTS TD-LTE, FWHE	472939A
Flexi Zone BTS TD-LTE, FWHF	472940A
Flexi Zone BTS TD-LTE, FWNA	473152A
Flexi Zone BTS TD-LTE, FWNB	473153A
Flexi Zone BTS TD-LTE, FWNC	473154A
Flexi Zone BTS TD-LTE, FWND	473122A
Flexi Zone BTS TD-LTE, FWHD	472852A
Flexi Zone BTS TD-LTE, FWHT (FB)	473531A
Flexi Zone BTS TD-LTE, FWHT (LB)	473737A
Flexi Zone BTS TD-LTE, FWHT (HB)	473738A
Flexi Zone BTS TD-LTE, FWHR (FB)	473548A
Flexi Zone BTS TD-LTE, FWHR (LB)	473603A
Flexi Zone BTS TD-LTE, FWHR (HB)	473604A
Flexi Zone BTS, FWGB	472851A
Flexi Zone BTS, FWIB	472899A
Flexi Zone BTS, FWHA	472897A
Flexi Zone BTS, FWFA	473040A
Flexi Zone BTS, FWEA	472898A
Flexi Zone BTS, FWHN	473148A
Flexi Zone BTS, FWHO	473149A
Flexi Zone BTS, FWEB	472941A
Flexi Zone BTS, FWIC	472942A
Flexi Zone BTS, FWID	473150A
Flexi Zone BTS, FWIE	473151A
Flexi Zone BTS, FWHC	472938A
Flexi Zone BTS, FWHG	472945A
Flexi Zone BTS, FWHH	472946A
Flexi Zone BTS, FWHI	473143A
Flexi Zone BTS, FWGI	473140A
Flexi Zone BTS, FWGJ	473141A
Flexi Zone BTS, FWGK	473142A
Flexi Zone BTS, FWFB	473041A
Flexi Zone BTS, FWFC	473138A
Flexi Zone BTS, FWFD	473139A
Flexi Zone BTS, FWEC	473135A
Flexi Zone BTS, FWED	473136A
Flexi Zone BTS, FWEE	473137A
Flexi Zone BTS, FWHM	473147A

3. COMPATIBILITY

Restore factory settings – RFSToolv4 supports a variety of BTS HW modules.
‘*And later*’ means any SW release published after BTS SW listed in the table (column – Target BTS SW). RFSToolv4 replaces all RFSToolv3 versions.

3.1 Flexi Multiradio and AirScale System Modules

RFSToolv4 2.10					
Module	**Unit (sub-unit)**	**Active BTS SW RAT**	**Target BTS SW RAT**	**Target BTS SW Version (and later)**	**Restore supported**
Flexi Multiradio 10 System Module	FSMF (FTIF) (FBBA) (FBBC)	WCDMA LTE TD-LTE SRAN GSM FDSW [4,5]	FDSW [6] WCDMA LTE TD-LTE SRAN	FDSW1.3 [6] FDSW2.0 [7] WN7.0 3.0 LN4.0 LNT2.0 SRAN16.2 1.0	YES
			GSM	-	NO [3]
	FSIH (FBIH)	TD-LTE FDSW	TD-LTE	FDSW2.0 [7] LNT4.0	YES
	FSMFA (FBBCA)	FDSW [9] LTE SRAN	LTE SRAN FDSW [8]	FL16A SRAN16.10	YES
Flexi Multiradio System Module	FSME FSMD FSMC	WCDMA [12] WN9.1 and later	WCDMA	WN9.1	YES
				WN9.0	NO [2]
			LTE	LN4.0	NO [2]
		WCDMA WN6.0 - WN9.0	WCDMA	WN9.1	NO [2]
				WN6.0 …WN9.0	YES
			LTE	LN4.0	NO [2]
	FSME	LTE [10]	WCDMA	WN6.0	NO [1]
			WCDMA	WN9.1	NO [1,2]
			LTE	LN4.0	YES
AirScale System Module	ASIA (ABIA)	FDSW [7] LTE TD-LTE SRAN	FDSW [7] LTE TD-LTE SRAN	FDSW2.0 [7] FL16A TL16A SRAN17A	YES
	ASIAA (ABIA)	FDSW [11] LTE	FDSW [11] LTE	FDSW2.1 [11] FL16A	

[1] SW updates are supported with RFSToolv2. Contact your local Nokia support.
[2] SW updates are supported with BTS Site manager. Refer to chapter 8.6.5.
[3] SW updates are supported with BTS Site manager. Refer to chapter 0.
[4] FDSW1.0 = FDSW1.0_RP_FD1405_310_00. Working only with RL70.
[5] FDSW1.1 = FDSW1.0_RP_FD1405_317_00. Added support for SW upgrade path to target BTS SW in FL15A and later / TL15A and later / SBTS16.2 and later as well to other RAT SWs.
[6] FDSW1.3 = FDSW1.3_RP_FD1405_327_00. Added support for SW upgrade path from SBTS16.2 and SBTS16.10 SW to SRAT SW (LTE/WCDMA/GSM) with FDSW as temporary middle step.
[7] FDSW2.0 = LN_WN_FDSW20_013.
[8] FDSW1.4 = FDSW1.4_RP_FD1405_330_00.
[9] FDSW1.2 = FDSW1.2_RP_FD1405_325_00.
[10] All loads + LN3.0_ENB_1103_771_02 as FSME A.11x factory delivery SW.
[11] FDSW2.1 = LN_WN_FDSW20_R4_TRUNK_502.

[4],[5],[6],[8],[9],[11] Refer to TS-SRAN-HW-0108.

Note: [12] Do not use RFSToolv4 for WCDMA FSME to clear Licensing info. Use RFSToolv3. Contact your local Nokia support. Correction is pending.

3.2 Flexi Zone BTS and others

RFSToolv4 2.10					
Module	**Unit (sub-unit)**	**Active BTS SW RAT**	**Target BTS SW RAT**	**Target BTS SW Version**	**Restore supported**
Flexi Zone BTS	FWGL, FWGM FWGN, FWFE FWFF, FWFG FWFI, FWGP	WCDMA LTE	WCDMA LTE	WZ9.1 / FLF15 / WBTSZ17 and later	YES
	FWNA, FWNB FWNC, FWND FWHD, FWHT FWHR	TD-LTE	TD-LTE	LNZ5.0 1.0 and later	YES
	FWHE, FWHF	TD-LTE	TD-LTE	LNZ5.0 and later	YES
	FWGB, FWIB FWHA	LTE	LTE	LNF5.0 and later	YES
	FWEB, FWIC FWID, FWIE FWHC, FWHG FWHH, FWHI	LTE	LTE	LNF7.0 and later	YES
	FWFA, FWEA FWHN, FWHO	LTE	LTE	LNF5.0 2.0 and later	YES
	FWGI, FWGJ FWGK, FWFB FWFC, FWFD FWEC,FWED FWEE, FWHM	LTE	LTE	LNF7.0 2.0 and later	YES
Flexi Multiradio EDGE System Module	ESMB ESMC	GSM	N/A	Configuration reset	NO
Flexi Lite BTS WCDMA	FQGA FQFA	WCDMA	WCDMA	WL7.0 2.0 and later	YES

3.3 Related features

Restore factory settings does not have directly any relation to listed feature ID's below. Any non-default password can be cleared using restore tool when password is known.

Feature ID	Feature name
RG302569	Remote BTS password management
RG302590	Remote BTS password management for GSM-R
RAN1210	Mass Updating of Local Flexi BTS Passwords via NetAct
RAN2504	Configurable Service Accounts
LTE1030	Configurable Service Account
LTE679	Local User account management
SR000906	SBTS Nokia Service Account Management
SR000900	SBTS Operator Account Management

4. KEYWORDS

Restore Factory Settings, System Module Recovery, RFSToolv4

5. TERMINOLOGY

The following terminology is used in this document:

ASIA	AirScale System Module Common
ABIA	AirScale System Module Capacity
FSMF	Flexi Multiradio 10 System Module
FSIH	Flexi Multiradio 10 System Module Indoor
FTIF	Transport sub-module (for FSMF)
FBBA	Extension baseband sub-module (for FSMF)
FBBC	Extension baseband sub-module (for FSMF)
FBIH	Extension baseband sub-module (for FSIH)
FQxx	Flexi Lite BTS WCDMA
FWxx	Flexi Zone BTS
FSMx	FSMF, FSME, FSMD, FSMC Flexi System Module
RFM	Flexi Multiradio RF module / Remote Radio head
FSM	Flexi System Module / target unit
RAT	Radio Access Technology
SRAN	Single RAN

6. WHEN SHOULD THIS TOOL BE USED?

6.1 Scenarios where system module recovery tool can help

Restore procedure is expected to recover all fault states described below, unless they are not caused by more severe fault e.g. HW failure in a FSM module/subunit.

1) A problem happened during installation/commissioning phase when new/replacement unit has been installed to network

Recovery procedure will replace existing BTS configuration database and will update BTS SW to FSM module. There is no need to remove FSM from BTS Site to attempt recovery.

2) BTS Site Manager connection cannot be established

Recovery procedure will remove existing configuration and database files and will upload new ones during recovery scenario. BTS will be restarted with new information.

3) SW mismatches between different Flexi BTS HW modules. SW download progress may not start at all or is partly downloaded to BTS but not completely. BTS SW will refuse to allow any further actions. Power may have been switched off-on between upgrade attempts and BTS cannot fully recover

Recovery procedure removes existing BTS SW configuration and will upload and flash new BTS SW files to FSM memory.

4) Commissioning steps cannot be successfully completed. BTS cannot become operational with normal re-commissioning steps. Active SCF file may prevent further re-commissioning attempts or some Flexi BTS module cannot reach operational state or there is a fake Flexi BTS module visible

Saving backup commissioning file is highly recommended. Recovery procedure removes existing hardware configuration and site commissioning file(s). FSM and whole BTS s set to not commissioned state.

5) FSM cannot be reused in another BTS site due to existing site configuration and licensing configuration

Optionally restore tool can remove existing Target Id and the related Last Used Timestamp -value from FSM. After network protocol time is retrieved to BTS, new Target Id value is generated for FSM unit.

6) FSM needs to be reused in another technology

Restore tool can perform a SW update to another BTS SW technology within minutes (if applicable).

7) Remove non-default local account settings

Restore tool can set local account to default settings (Nemuadmin/nemuuser). In addition, password management functionality can be used to remove non-default local account settings. See chapter 6.4 for further details.

8) Remove non-default service account settings

Restore tool can set service account to default settings (toor4nsn). In addition, password management functionality can be used to remove non-default service account settings. See chapter 6.4 for further details.

9) Restore operator certificates

Restore tool can remove operator certificates from active and/or passive partition to prepare target unit to start over Plug and Play scenario. Additionally, for example in LTE=>SRAN migration scenario, BTS configuration files can be removed in addition to certificate removal.

10) Simple upgrade

Replacement/spare FSM may need to be updated over the number of system releases to reach target SW release. Restore tool can provide the same in one attempt to step forward in BTS, for example WN7.0 to WN9.0 (WCDMA FSME) and RL70 to FL16 (LTE FSME).

11) Introduce configuration reset (clear FSM role)

Restore tool can perform configuration reset when full recovery scenario is executed. For example, FSMF used in LTE, the FSM role is cleared while SW update to WCDMA is made.

Note: No Ethernet cable shall be connected to LMP port in extension system module when it is connected to master system module. Otherwise FSM cannot achieve extension module role.

Configuration reset deletes the existing configuration data and clears the System Module role. The process can be also performed by pressing and holding the reset button. The button is located next to the EIF1 interface on the front panel.
- Press and hold reset button for at least five seconds and release reset button and then press reset button another time quickly and identify that FSMF is prepared to restart (*EIF1*, *FAN*, *STATUS* LED’s are shortly blinking red).

Note: In extension module configurations, FSMF might have a problem with FSM role and therefore does not provide ping response. To remove possible misconfiguration, issue a configuration reset as detailed above and depending on the ping response, recovery routine can be attempted.

12) Introduce SW rollback

Restore tool can perform SW rollback in case active product SW does not support it. This functionality is available for FSMF, FSIH, FQGA and FQFA.

13) Install FDSW

Restore tool can install FDSW on top of any active product SW version.

6.2 Scenarios where restore factory setting should not be used

1) No ping response from target unit. Restore procedure cannot login to unit

Unit ping response is required from one if the IP addresses: 192.168.255.1, 192.168.255.5, 192.168.255.7, 192.168.255.16, 192.168.255.119, 192.168.255.127, 192.168.255.129 or 192.168.255.131. Restore tool is requesting ping response to attempt connection.

2) Fault ID is reported that can be connected to more severe failure

Refer to existing BTS alarm documentation / BTS Site Manager Online Help for further information on BTS fault descriptions and to be able identify fault ID's that are caused by real HW failure.

3) Fault ID is reported again and BTS functionality / service is affected despite of successful recovery

Since restore application does not make analysis during FSM during recovery session, it is possible that problem situation can reproduce after FSM unit has been once restored. In this case further troubleshooting activities are needed to identify possible product SW problem / HW failure. The following problems cannot be fixed with restore tool:

FSME/D/C

1)	BTS autonomous reset as recovery action	(Fault ID: 10)
2)	System module failure	(Fault ID: 412)
3)	System module failure	(Fault ID: 418)
4)	System module failure	(Fault ID: 69)
5)	Unit autonomous reset as recovery action	(Fault ID: 4019)
6)	BTS internal SW management problem	(Fault ID: 0214)
7)	Baseband bus failure	(Fault ID: 1811)
8)	BTS internal SW management problem	(Fault ID: 6)

FSMF/FSIH

1)	BTS autonomous reset as recovery action	(Fault ID: 10)
2)	System module failure	(Fault ID: 10)
3)	Firmware SW mismatch	(Fault ID: 2056)

Application does not make analysis on reported alarm history or events store to FSM unit. Restore procedure may be concluded successfully. However, it is likely that the more severe fault state may not recover. FSM unit is set to factory settings only from SW management point of view.

6.3 How long it takes

The total time needed for recovery procedure depends on the number of files to be uploaded to FSM unit. Typical recovery time for ASIA/FSMF/FQxx/FWxx units is from 2 to 6 minutes and for FSME in WCDMA less than 9 minutes and in LTE approximately 16 minutes. For FWxx modules procedure takes less than 2 minutes.

- Varying amount and size of files to be deleted and uploaded.
- Difference in storing new files due to varying flash memory hardware

Note: The SW activation of new target SW may take up to 15 minutes with FSMF and multiple resets can be observed.

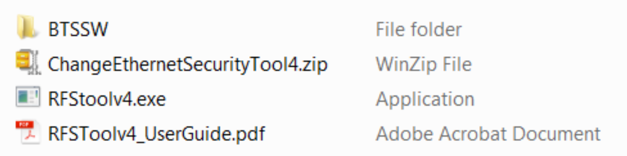
Make sure that RFS tool can execute completely without any interruptions. In case of accidentally interrupted session it is anyway worth trying again.

Switching power off-on between attempts may cause unrecoverable condition to system module.

7. INITIAL SETUP

7.1 Install restore tool

Unzip restore tool delivery package to local directory.

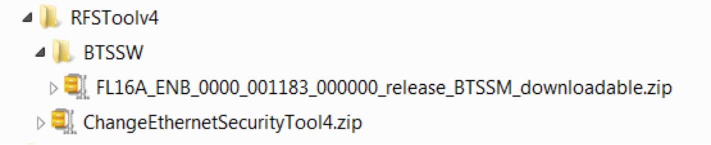


BTSSW	File folder
ChangeEthernetSecurityTool4.zip	WinZip File
RFStoolv4.exe	Application
RFSToolv4_UserGuide.pdf	Adobe Acrobat Document

If another version already exists, no need to remove it.

7.2 Download & Setup of BTS Software

Download the BTS software and store it to your local PC such as C:\Temp.
Store target BTS SW to \RFSToolv4\BTSSW. Multiple loads can be placed to same folder.



```
◢ RFSToolv4
  ◢ BTSSW
    ▷ FL16A_ENB_0000_001183_000000_release_BTSSM_downloadable.zip
  ▷ ChangeEthernetSecurityTool4.zip
```

Restore tool extracts automatically the required files from given BTS SW package.

7.3 Configure PC Ethernet adapter with static IP for local connectivity

Select parameters to enable local connection to BTS.

Technology	PC Host IP	PC Subnet Mask
GSM ESMB/ESMC	192.168.255.126	255.255.0.0
2G FSMF	192.168.255.130	255.255.0.0
WCDMA (any)	192.168.255.126	255.255.0.0
TD-LTE (any)	192.168.255.126	255.255.0.0
LTE (any)	192.168.255.126	255.255.0.0
SRAN (any)	192.168.255.126	255.255.0.0

Note: You may need to disable/enable the network adapter to make sure the settings are applied. This can be verified under Start -> Run -> cmd.exe and executing ‘ipconfig /all’

1) **Connect to BTS locally via LMP**

IP for location connection, for example: 192.168.255.129

2) **Backup the SCF via BTS Manager**

This file will be used if the site needs to be recommissioned for any reason.

3) **Close the BTS Manager application**

Active BTS Site manager connection cannot be running while restore tool is communicating with target BTS.

7.4 Password management

Password management provides a method to remove non-default local account and service account settings to enable FSM reuse, failure screening and service operations. Password management is automatically enabled in case default Local account and/or service account credentials do not work.

In case user can provide needed credentials, the removal of changed settings can be done without deploying encrypted password file in use. If user is not aware of changed local and/or service account settings, the authority who is to coordinate the password management in the network shall provide an encrypted file including working credentials and furthermore needed service operations can be smoothly completed.

Encrypted password management functionality enables sharing the local and service account credentials in encrypted format which cannot be read from the file (in ASCII format). Secured connection is then used to remove local account and service account settings.

7.4.1 Password encryption

Restore factory settings shall be supplied with ASCII formatted file including several login/password information. This information is then introduced to restore tool that processes the encryption and creates a file (ASCII formatted). File is ready to be shared.

Password file formed with RFSToolv3 is compatible with RFSToolv4.

The following steps are needed to form an encrypted password file.

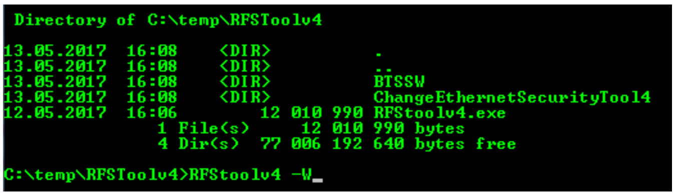
STEP 1

- Open for example ‘Notepad’ and enter several login and passwords pair(s).
- Include all actual usernames and passwords that need to be encrypted. Add ‘:’ between username and password in each line. In total 99 pairs of username/password(s) are accepted to one password file.
- Save file as ‘pws.txt’ to restore tool root directory e.g. `C:\temp\RFSToolv4\pws.txt.`

```
#An example of pws.txt each line put one actual username:password
toor4nsn:password1
toor4nsn:password2
Nemuadmin:password4
Nemuadmin:password5
...
```

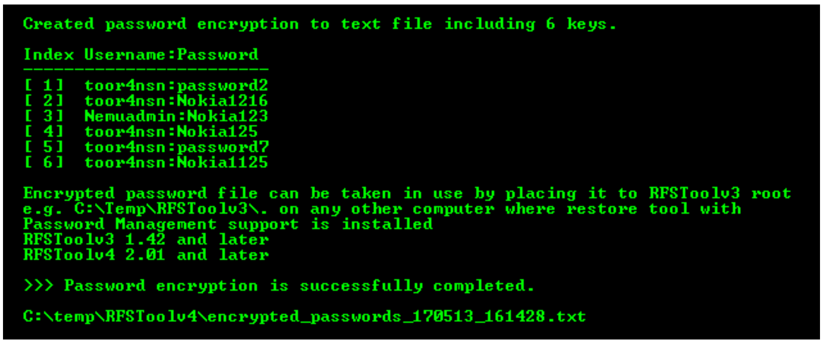
STEP 2

- Open command window to restore tool root directory, e.g. `C:\temp\RFSToolv4`
- Start restore tool with the command line option: `C:\temp\Rfstoolv4.exe -W`
  Note: Encrypted password management scenario is started only when ‘pws.txt’ file is in restore tool root directory. One file is taken in use at a time.



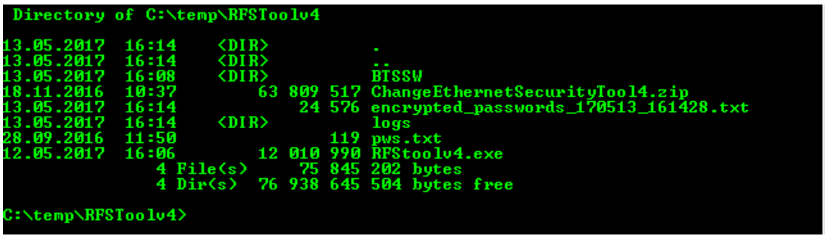
```
 Directory of C:\temp\RFSToolv4

13.05.2017  16:08    <DIR>          .
13.05.2017  16:08    <DIR>          ..
13.05.2017  16:08    <DIR>          BTSSW
13.05.2017  16:08    <DIR>          ChangeEthernetSecurityTool4
12.05.2017  16:06        12 010 990 RFStoolv4.exe
               1 File(s)     12 010 990 bytes
               4 Dir(s)  77 006 192 640 bytes free

C:\temp\RFSToolv4>RFStoolv4 -W_
```

- Observe processed username and password pairs that are displayed by restore tool. Up to 99 pairs are displayed, the rest are not taken in account.
  Note: No information is collected at any point of restore procedure about encrypted usernames and passwords.



```
Created password encryption to text file including 6 keys.

Index Username:Password
-------------------------
[ 1]  toor4nsn:password2
[ 2]  toor4nsn:Nokia1216
[ 3]  Nemuadmin:Nokia123
[ 4]  toor4nsn:Nokia125
[ 5]  toor4nsn:password7
[ 6]  toor4nsn:Nokia1125

Encrypted password file can be taken in use by placing it to RFSToolv3 root
e.g. C:\Temp\RFSToolv3\. on any other computer where restore tool with
Password Management support is installed
RFSToolv3 1.42 and later
RFSToolv4 2.01 and later

>>> Password encryption is successfully completed.

C:\temp\RFSToolv4\encrypted_passwords_170513_161428.txt
```

Encrypted password information is saved to restore tool root directory,
e.g. `C:\temp\RFStoolv4\encrypted_passwords_160822_140815.txt`

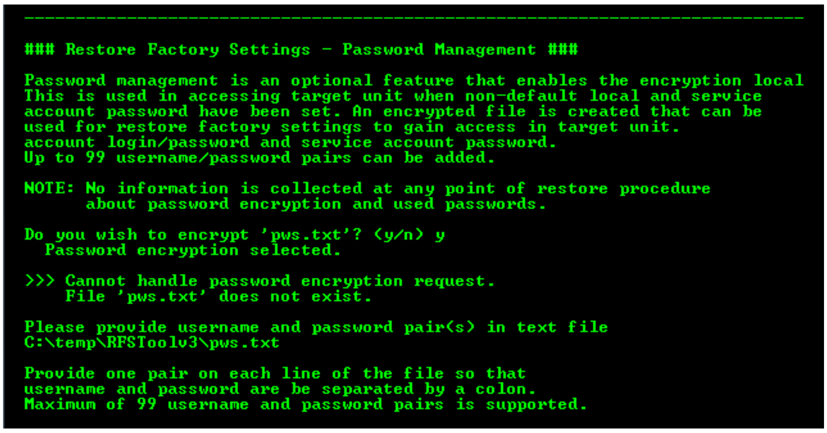


```
 Directory of C:\temp\RFSToolv4

13.05.2017  16:14    <DIR>          .
13.05.2017  16:14    <DIR>          ..
13.05.2017  16:08    <DIR>          BTSSW
18.11.2016  10:37        63 809 517 ChangeEthernetSecurityTool4.zip
13.05.2017  16:14            24 576 encrypted_passwords_170513_161428.txt
13.05.2017  16:14    <DIR>          logs
28.09.2016  11:50               119 pws.txt
12.05.2017  16:06        12 010 990 RFStoolv4.exe
               4 File(s)     75 845 202 bytes
               4 Dir(s)  76 938 645 504 bytes free

C:\temp\RFSToolv4>
```

'Encrypted_password_ddmmyy_hhmmss.txt' file can be renamed for better identification for example like this:
`C:\temp\RFStoolv4\encrypted_passwords_160822_140815_CLUSTER_80.txt`

Note: Encrypted password file cannot be decrypted to readable format by using restore tool. When encrypted file is introduced to restore tool, username and password information is decrypted to internal database for the time of restore procedure. Restore tool log files does not include direct information of encrypted usernames and passwords. Tool does identify when encrypted scenario shall be deployed but no used usernames or password are stored to log file. Neither user is prompted which encrypted credentials are used.
In case 'pws.txt' does not exist in root directory, user is prompted to provide one.

In case ‘pws.txt’ does not exist in root directory, user is prompted to provide one.



```
---------------------------------------------------------------------------

### Restore Factory Settings - Password Management ###

Password management is an optional feature that enables the encryption local
This is used in accessing target unit when non-default local and service
account password have been set. An encrypted file is created that can be
used for restore factory settings to gain access in target unit.
account login/password and service account password.
Up to 99 username/password pairs can be added.

NOTE: No information is collected at any point of restore procedure
      about password encryption and used passwords.

Do you wish to encrypt 'pws.txt'? (y/n) y
  Password encryption selected.

>>> Cannot handle password encryption request.
    File 'pws.txt' does not exist.

Please provide username and password pair(s) in text file
C:\temp\RFSToolv3\pws.txt

Provide one pair on each line of the file so that
username and password are be separated by a colon.
Maximum of 99 username and password pairs is supported.
```

7.4.2 Encrypted password file usage

RFSToolv3 version 1.42 / RFSToolv4 version 2.01 and above is supporting the use of encrypted password file.

Encrypted password management is automatically started when restore tool is equipped in encrypted password files(s) ‘encrypted_passwords_ddmmyy_hhmmss.txt’ and if procedure cannot gain access to FSM with default username/password information. There can be one or many files at the same time. Restore tool is browsing through the root directory files after the procedure is started. All files that match to naming convention ‘encrypted_passwords_ddmmyy_hhmmss.txt’ are displayed to user. Only one file however can be taken in use at a time.

7.4.3 Removing Service account settings

In case of FSME/D/C (both in WCDMA and LTE), restore procedure requires more time to process the necessary steps. Whenever service account settings are removed using SSH connections, FSM is reset to gain access with default service account username and password (Nokia credentials). With other modules Service account settings are removed during complete restore procedure.

7.4.4 Removing Local account settings

In case of FSME/D/C (both in WCDMA and LTE), ‘Recover FTM’ functionality needs to be selected during restore procedure to get local account settings removed. With other modules Local account settings are removed during complete restore procedure.

8. RESTORE FACTORY SETTINGS OF SYSTEM MODULE

In the following chapters, the common steps of restore procedure and RAT SW specific steps are described. Chapter 8.1 is valid for all FSM modules supported and latter chapters have details for unit specific scenarios.

8.1 Procedure – common preparations

1) CHECK TARGET BTS SW AVAILABILITY IN \BTSSW\ FOLDER

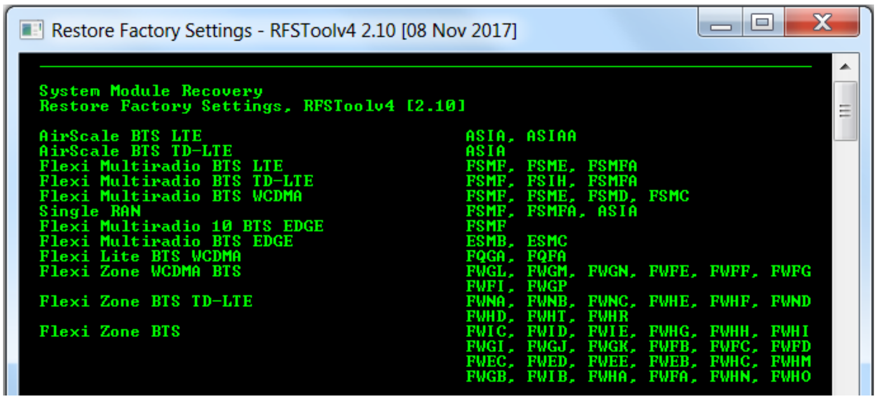
As described in chapter 7.2, make sure needed target SW is placed to \BTSSW\ folder under restore tool root directory.

2) INTRODUCE PASSWORD FILE (optional)

This step is optional, and is meant to guide in password management scenario. Place encrypted password file 'encrypted_passwords_ddmmyy_hhmmss.txt' to restore tool root directory, e.g. `C:\Temp\RFSToolv4`. Check chapter 7.4 how to obtain encrypted password file.

3) LAUNCH APPLICATION

Start application 'RFSToolv4.exe' in restore tool root directory, e.g. `C:\Temp\RFSToolv4`. Observe used application version.



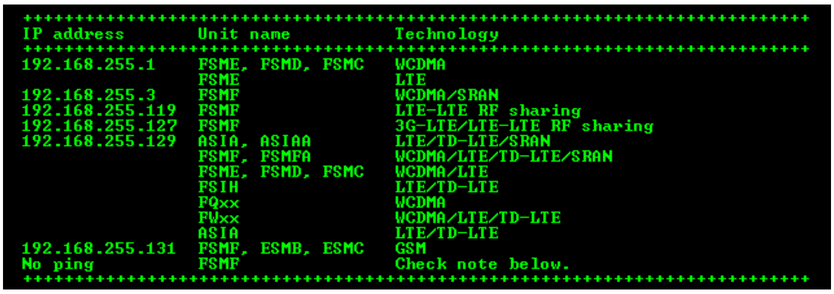
Restore Factory Settings - RFSToolv4 2.10 [08 Nov 2017]

```
System Module Recovery
Restore Factory Settings, RFSToolv4 [2.10]

AirScale BTS LTE                        ASIA, ASIAA
AirScale BTS TD-LTE                     ASIA
Flexi Multiradio BTS LTE                FSMF, FSME, FSMFA
Flexi Multiradio BTS TD-LTE             FSMF, FSIH, FSMFA
Flexi Multiradio BTS WCDMA              FSMF, FSME, FSMD, FSMC
Single RAN                              FSMF, FSMFA, ASIA
Flexi Multiradio 10 BTS EDGE            FSMF
Flexi Multiradio BTS EDGE               ESMB, ESMC
Flexi Lite BTS WCDMA                    FQGA, FQFA
Flexi Zone WCDMA BTS                    FWGL, FWGM, FWGN, FWFE, FWFF, FWFG
                                        FWFI, FWGP
Flexi Zone BTS TD-LTE                   FWNA, FWNB, FWNC, FWHE, FWHF, FWND
                                        FWHD, FWHT, FWHR
Flexi Zone BTS                          FWIC, FWID, FWIE, FWHG, FWHH, FWHI
                                        FWGI, FWGJ, FWGK, FWFB, FWFC, FWFD
                                        FWEC, FWED, FWEE, FWEB, FWHC, FWHM
                                        FWGB, FWIB, FWHA, FWFA, FWHN, FWHO
```

RFS application requires a temporary folder for file handling and for collecting & storing log files. If e.g. `C:\Temp\RFSToolv4\logs` cannot be found, `\logs` is created during first time use.

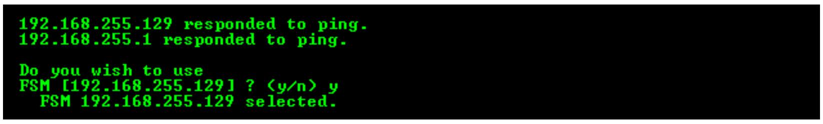
4) CHECK BTS CONFIGURATION

Restore tool will automatically find out available hosts. The list of IP addresses supported is used to find ping response from target host.



```
*****************************************************************************
IP address        Unit name           Technology
*****************************************************************************
192.168.255.1     FSME, FSMD, FSMC    WCDMA
                  FSME                LTE
192.168.255.3     FSMF                WCDMA/SRAN
192.168.255.119   FSMF                LTE-LTE RF sharing
192.168.255.127   FSMF                3G-LTE/LTE-LTE RF sharing
192.168.255.129   ASIA, ASIAA         LTE/TD-LTE/SRAN
                  FSMF, FSMFA         WCDMA/LTE/TD-LTE/SRAN
                  FSME, FSMD, FSMC    WCDMA/LTE
                  FSIH                LTE/TD-LTE
                  FQxx                WCDMA
                  FWxx                WCDMA/LTE/TD-LTE
                  ASIA                LTE/TD-LTE
192.168.255.131   FSMF, ESMB, ESMC    GSM
No ping           FSMF                Check note below.
*****************************************************************************
```

When 2 consecutive ping responses are received, ping scenario is stopped and user shall select and confirm to continue.



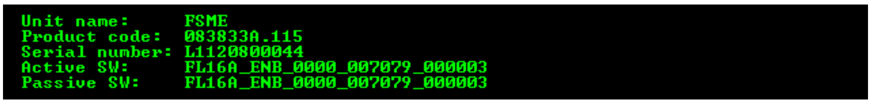
```
192.168.255.129 responded to ping.
192.168.255.1 responded to ping.

Do you wish to use
FSM [192.168.255.129] ? (y/n) y
  FSM 192.168.255.129 selected.
```

Restore tool is attempting TCP connections with default local and service account settings. Refer to chapter 7.4 when these settings are not known/not available.

With FSMF, if no ping response or unit is in extension module role - use reset button under EIF1 port to remove BTS configuration/extension module role. Press 10 seconds then wait 2 minutes, and reset FSM module to finish the clearing procedure.

5) DATA COLLECTION FROM BTS

This will open temporary TCP connections to BTS. Restore tool is automatically fetching the data from FSM. The progress of creating connections and found information is displayed.



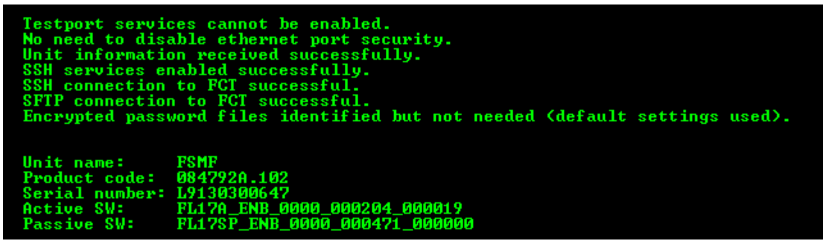
```
Unit name:      FSME
Product code:   083833A.115
Serial number:  L1120800044
Active SW:      FL16A_ENB_0000_007079_000003
Passive SW:     FL16A_ENB_0000_007079_000003
```

Note: BTS Site manager connection cannot be active at the same time to target BTS. Close active BTS Site manager connection. Close restore tool and try again.

8.2 Procedure – preparations FSMF/FSMFA/FSIH

1) DATA COLLECTION FROM FSMF

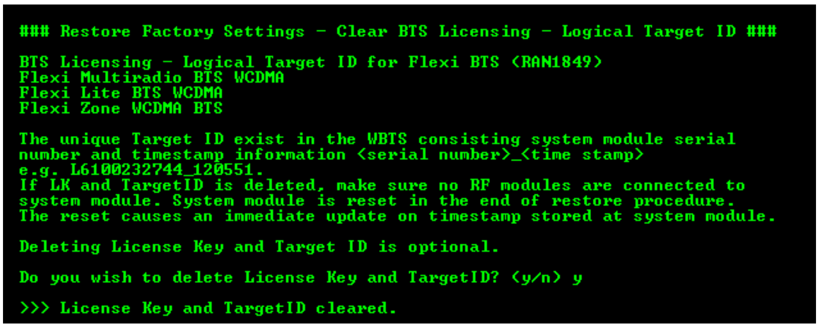
The progress of required connections made, unit and SW version information found is displayed.



```
Testport services cannot be enabled.
No need to disable ethernet port security.
Unit information received successfully.
SSH services enabled successfully.
SSH connection to FCT successful.
SFTP connection to FCT successful.
Encrypted password files identified but not needed (default settings used).


Unit name:     FSMF
Product code:  084792A.102
Serial number: L9130300647
Active SW:     FL17A_ENB_0000_000204_000019
Passive SW:    FL17SP_ENB_0000_000471_000000
```

2) DELETE LICENSE KEY – TARGET ID [WCDMA] (optional)

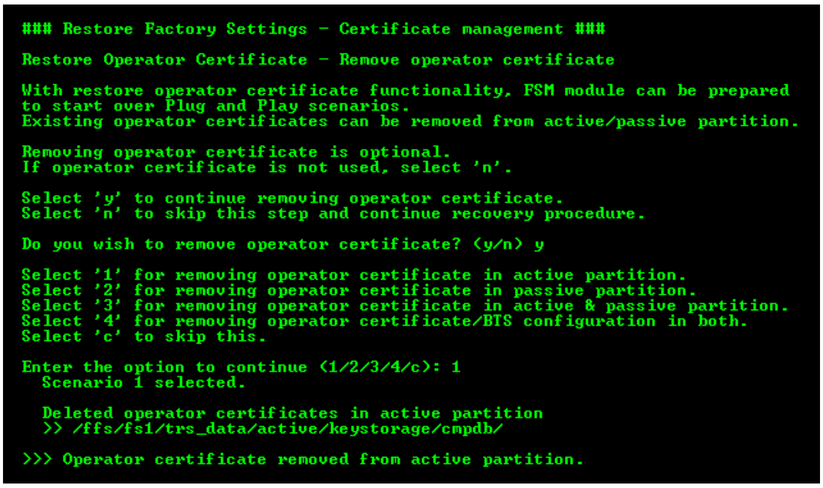
If license keys and Target ID are chosen to be deleted and FZM module is reset in the end of restore procedure, the reset causes an immediate update on timestamp stored at system module.



```
### Restore Factory Settings - Clear BTS Licensing - Logical Target ID ###

BTS Licensing - Logical Target ID for Flexi BTS (RAN1849)
Flexi Multiradio BTS WCDMA
Flexi Lite BTS WCDMA
Flexi Zone WCDMA BTS

The unique Target ID exist in the WBTS consisting system module serial
number and timestamp information (serial number>_<time stamp>
e.g. L6100232744_120551.
If LK and TargetID is deleted, make sure no RF modules are connected to
system module. System module is reset in the end of restore procedure.
The reset causes an immediate update on timestamp stored at system module.

Deleting License Key and Target ID is optional.

Do you wish to delete License Key and TargetID? (y/n) y

>>> License Key and TargetID cleared.
```

3) DELETE OPERATOR CERTIFICATE (optional)

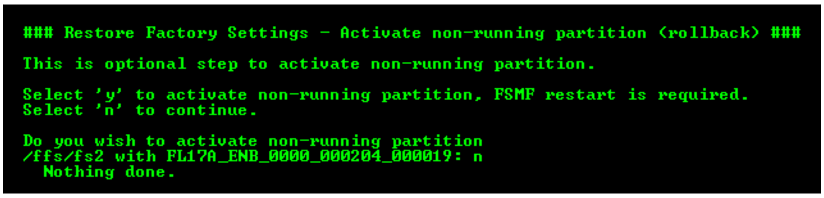
Operator certificates from active and/or passive partition to prepare target unit to start over Plug and Play scenario. Select preferred option to remove operator certificate.



```
### Restore Factory Settings - Certificate management ###

Restore Operator Certificate - Remove operator certificate

With restore operator certificate functionality, FSM module can be prepared
to start over Plug and Play scenarios.
Existing operator certificates can be removed from active/passive partition.

Removing operator certificate is optional.
If operator certificate is not used, select 'n'.

Select 'y' to continue removing operator certificate.
Select 'n' to skip this step and continue recovery procedure.

Do you wish to remove operator certificate? (y/n) y

Select '1' for removing operator certificate in active partition.
Select '2' for removing operator certificate in passive partition.
Select '3' for removing operator certificate in active & passive partition.
Select '4' for removing operator certificate/BTS configuration in both.
Select 'c' to skip this.

Enter the option to continue (1/2/3/4/c): 1
  Scenario 1 selected.

  Deleted operator certificates in active partition
  >> /ffs/fs1/trs_data/active/keystorage/cmpdb/

>>> Operator certificate removed from active partition.
```

4) ACTIVATE NON-RUNNING PARTITION - SW ROLLBACK (optional)

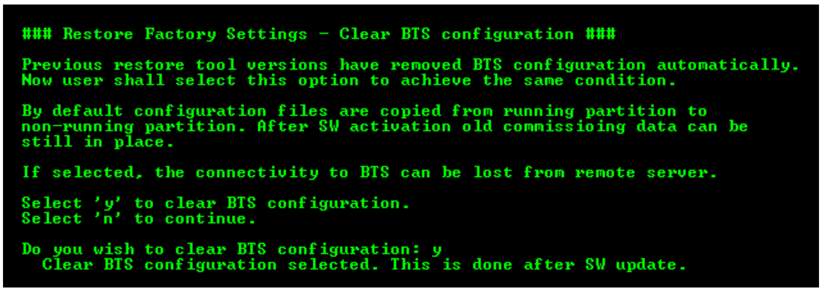
Non-running partition can be activated by choice. Select option to clear TRS/BTS configuration. FSM module restart is required to complete SW rollback scenario.



```
### Restore Factory Settings - Activate non-running partition (rollback) ###

This is optional step to activate non-running partition.

Select 'y' to activate non-running partition, FSMF restart is required.
Select 'n' to continue.

Do you wish to activate non-running partition
/ffs/fs2 with FL17A_ENB_0000_000204_000019: n
  Nothing done.
```

5) CLEAR BTS CONFIGURATION (optional)

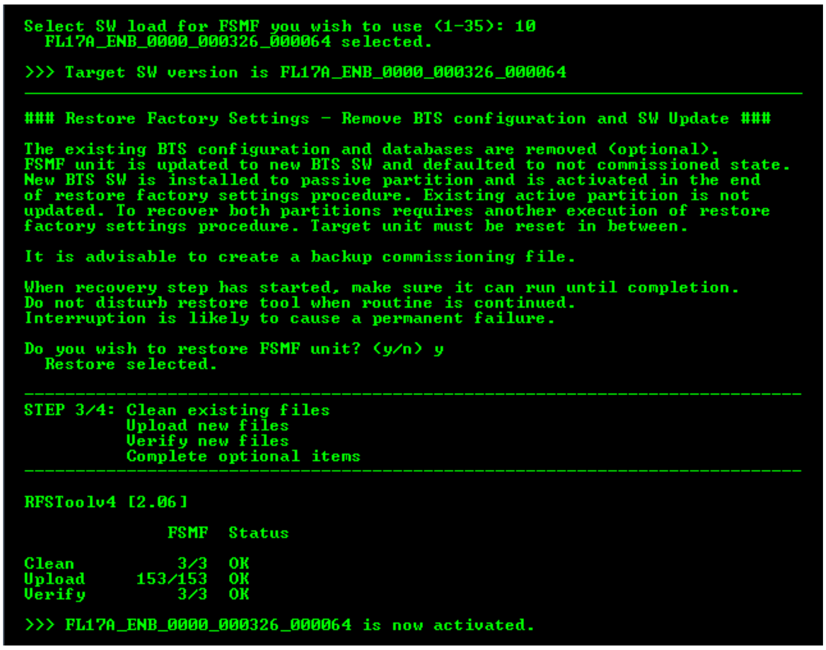
TRS/BTS configuration is not removed by default. Select option to clear TRS/BTS configuration. It will be done after SW update is completed.



```
### Restore Factory Settings - Clear BTS configuration ###

Previous restore tool versions have removed BTS configuration automatically.
Now user shall select this option to achieve the same condition.

By default configuration files are copied from running partition to
non-running partition. After SW activation old commissioing data can be
still in place.

If selected, the connectivity to BTS can be lost from remote server.

Select 'y' to clear BTS configuration.
Select 'n' to continue.

Do you wish to clear BTS configuration: y
  Clear BTS configuration selected. This is done after SW update.
```

6) SELECT SW RELEASE AND CONFIRM TO START

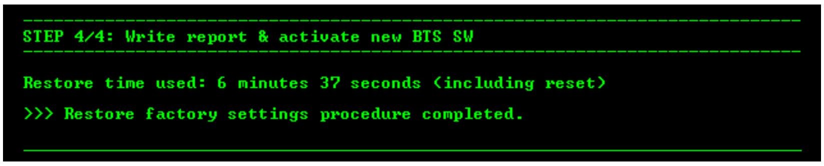
Select target SW from list (made of SW loads stored in \BTSSW\).
Confirm to start recovery procedure.



```
Select SW load for FSMF you wish to use (1-35): 10
  FL17A_ENB_0000_000326_000064 selected.

>>> Target SW version is FL17A_ENB_0000_000326_000064
____________________________________________________________________________

### Restore Factory Settings - Remove BTS configuration and SW Update ###

The existing BTS configuration and databases are removed (optional).
FSMF unit is updated to new BTS SW and defaulted to not commissioned state.
New BTS SW is installed to passive partition and is activated in the end
of restore factory settings procedure. Existing active partition is not
updated. To recover both partitions requires another execution of restore
factory settings procedure. Target unit must be reset in between.

It is advisable to create a backup commissioning file.

When recovery step has started, make sure it can run until completion.
Do not disturb restore tool when routine is continued.
Interruption is likely to cause a permanent failure.

Do you wish to restore FSMF unit? (y/n) y
  Restore selected.

----------------------------------------------------------------------------
STEP 3/4: Clean existing files
          Upload new files
          Verify new files
          Complete optional items
----------------------------------------------------------------------------

RFSToolv4 [2.06]

              FSMF  Status

Clean          3/3  OK
Upload     153/153  OK
Verify         3/3  OK

>>> FL17A_ENB_0000_000326_000064 is now activated.
```

7) CLOSE APPLICATION & OBSERVE LOG FILE

FSM module is automatically restarted to take new SW in use.
System module can take additional resets before full SW activation is completed.



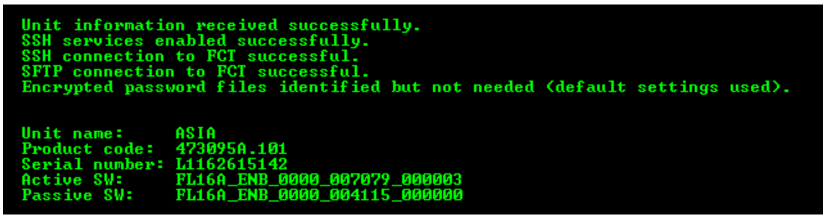
```
--------------------------------------------------------------------------------
STEP 4/4: Write report & activate new BTS SW
--------------------------------------------------------------------------------

Restore time used: 6 minutes 37 seconds (including reset)

>>> Restore factory settings procedure completed.

________________________________________________________________________________
```

After each execution, a report file in txt format is created that is significant to each system module based on the serial number and current date/time. RFS report file name is specified by the serial number, product code, current date and time (e.g. C:\Temp\RFSToolv4\logs\ L6130705629_084792A.101_ _20140902_143756.txt). RFS report is stored to \logs under restore tool root directory.

8.3 Procedure – preparations ASIA/ASIAA

1) DATA COLLECTION FROM ASIA

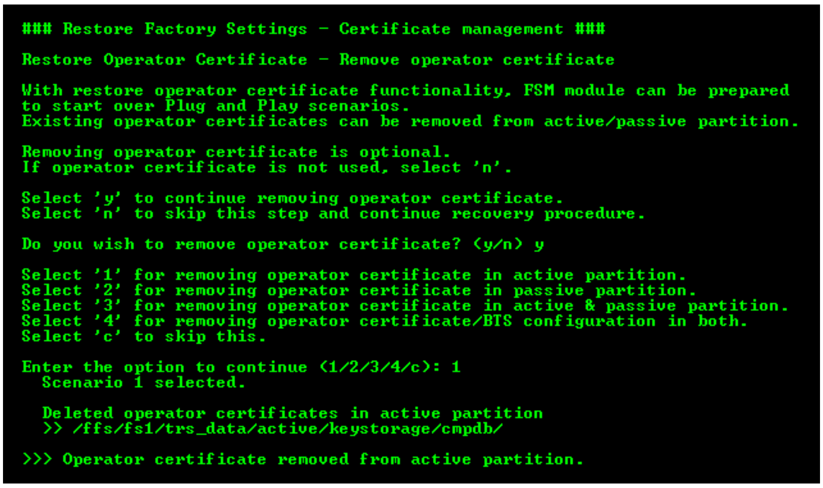
The progress of required connections, unit and SW version information found is displayed.



```
Unit information received successfully.
SSH services enabled successfully.
SSH connection to FCT successful.
SFTP connection to FCT successful.
Encrypted password files identified but not needed (default settings used).


Unit name:     ASIA
Product code:  473095A.101
Serial number: L1162615142
Active SW:     FL16A_ENB_0000_007079_000003
Passive SW:    FL16A_ENB_0000_004115_000000
```

2) DELETE OPERATOR CERTIFICATE (optional)

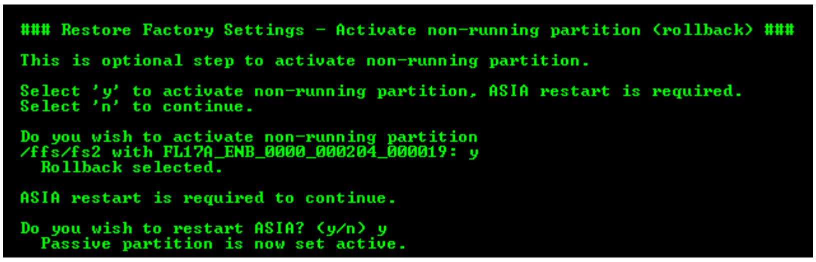
Operator certificates from active and/or passive partition to prepare target unit to start over Plug and Play scenario. Select preferred option to remove operator certificate.



```
### Restore Factory Settings - Certificate management ###

Restore Operator Certificate - Remove operator certificate

With restore operator certificate functionality, FSM module can be prepared
to start over Plug and Play scenarios.
Existing operator certificates can be removed from active/passive partition.

Removing operator certificate is optional.
If operator certificate is not used, select 'n'.

Select 'y' to continue removing operator certificate.
Select 'n' to skip this step and continue recovery procedure.

Do you wish to remove operator certificate? (y/n) y

Select '1' for removing operator certificate in active partition.
Select '2' for removing operator certificate in passive partition.
Select '3' for removing operator certificate in active & passive partition.
Select '4' for removing operator certificate/BTS configuration in both.
Select 'c' to skip this.

Enter the option to continue (1/2/3/4/c): 1
  Scenario 1 selected.

  Deleted operator certificates in active partition
  >> /ffs/fs1/trs_data/active/keystorage/cmpdb/

>>> Operator certificate removed from active partition.
```

3) ACTIVATE NON-RUNNING PARTITION - SW ROLLBACK (optional)

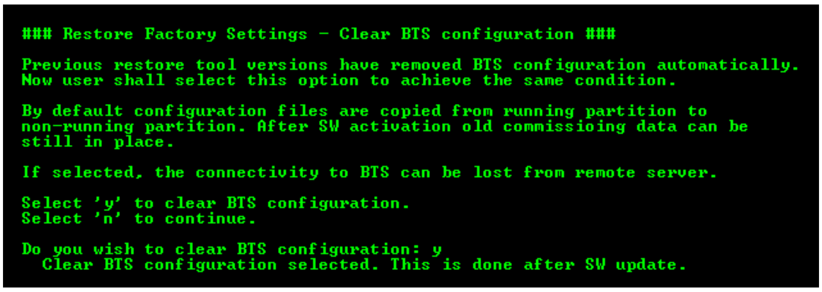
Non-running partition can be activated by choice. Select option to clear TRS/BTS configuration. FSM module restart is required to complete SW rollback scenario.



```
### Restore Factory Settings - Activate non-running partition (rollback) ###

This is optional step to activate non-running partition.

Select 'y' to activate non-running partition, ASIA restart is required.
Select 'n' to continue.

Do you wish to activate non-running partition
/ffs/fs2 with FL17A_ENB_0000_000204_000019: y
  Rollback selected.

ASIA restart is required to continue.

Do you wish to restart ASIA? (y/n) y
  Passive partition is now set active.
```

4) CLEAR BTS CONFIGURATION (optional)

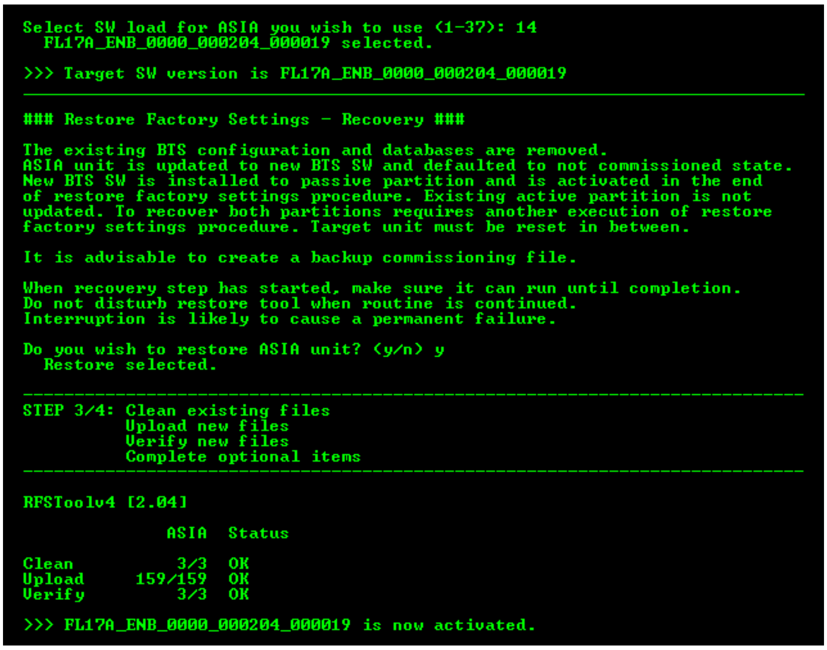
TRS/BTS configuration is not removed by default. Select option to clear TRS/BTS configuration.



```
### Restore Factory Settings - Clear BTS configuration ###

Previous restore tool versions have removed BTS configuration automatically.
Now user shall select this option to achieve the same condition.

By default configuration files are copied from running partition to
non-running partition. After SW activation old commissioing data can be
still in place.

If selected, the connectivity to BTS can be lost from remote server.

Select 'y' to clear BTS configuration.
Select 'n' to continue.

Do you wish to clear BTS configuration: y
  Clear BTS configuration selected. This is done after SW update.
```

5) SELECT SW RELEASE AND CONFIRM TO START

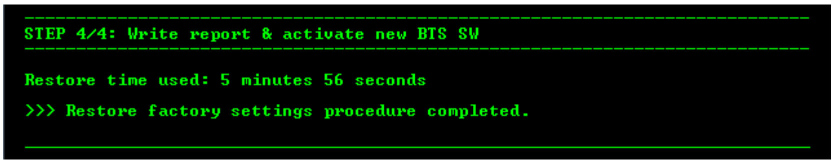
Select target SW from list (made of SW loads stored in \BTSSW\).
Confirm to start recovery procedure.



```
Select SW load for ASIA you wish to use (1-37): 14
  FL17A_ENB_0000_000204_000019 selected.

>>> Target SW version is FL17A_ENB_0000_000204_000019
______________________________________________________________________________

### Restore Factory Settings - Recovery ###

The existing BTS configuration and databases are removed.
ASIA unit is updated to new BTS SW and defaulted to not commissioned state.
New BTS SW is installed to passive partition and is activated in the end
of restore factory settings procedure. Existing active partition is not
updated. To recover both partitions requires another execution of restore
factory settings procedure. Target unit must be reset in between.

It is advisable to create a backup commissioning file.

When recovery step has started, make sure it can run until completion.
Do not disturb restore tool when routine is continued.
Interruption is likely to cause a permanent failure.

Do you wish to restore ASIA unit? (y/n) y
  Restore selected.

------------------------------------------------------------------------------
STEP 3/4: Clean existing files
          Upload new files
          Verify new files
          Complete optional items
------------------------------------------------------------------------------

RFSToolv4 [2.04]

              ASIA   Status

Clean          3/3   OK
Upload     159/159   OK
Verify         3/3   OK

>>> FL17A_ENB_0000_000204_000019 is now activated.
```

6) CLOSE APPLICATION & OBSERVE LOG FILE

ASIA module is automatically restarted to take new SW in use.
System module can take additional resets before full SW activation is completed.



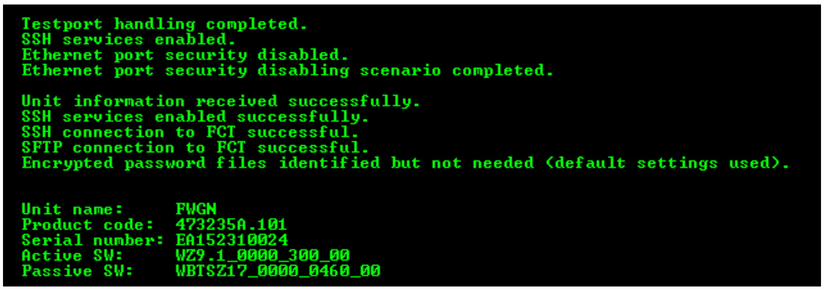
```
------------------------------------------------------------------------------
STEP 4/4: Write report & activate new BTS SW
------------------------------------------------------------------------------

Restore time used: 5 minutes 56 seconds

>>> Restore factory settings procedure completed.

______________________________________________________________________________
```

After each execution, a report file in txt format is created that is significant to each system module based on the serial number and current date/time. RFS report file name is specified by the serial number, product code, current date and time (e.g. C:\Temp\RFSToolv4\logs\ L6130705629_084792A.101_ _20140902_143756.txt). RFS report is stored to \logs under restore tool root directory.

8.4 Procedure – preparations FWxx

1) DATA COLLECTION FROM FLEXI ZONE BTS

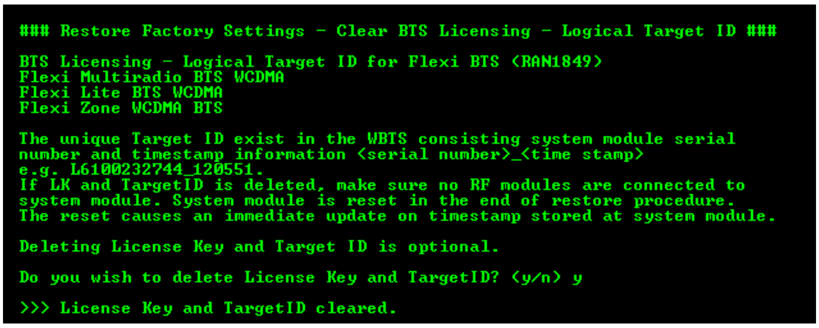
The progress of required connections, unit and SW version information found is displayed.



```
Testport handling completed.
SSH services enabled.
Ethernet port security disabled.
Ethernet port security disabling scenario completed.

Unit information received successfully.
SSH services enabled successfully.
SSH connection to FCT successful.
SFTP connection to FCT successful.
Encrypted password files identified but not needed (default settings used).


Unit name:     FWGN
Product code:  473235A.101
Serial number: EA152310024
Active SW:     WZ9.1_0000_300_00
Passive SW:    WBTSZ17_0000_0460_00
```

2) DELETE LICENSE KEY – TARGET ID [FLEXI ZONE BTS WCDMA] (optional)

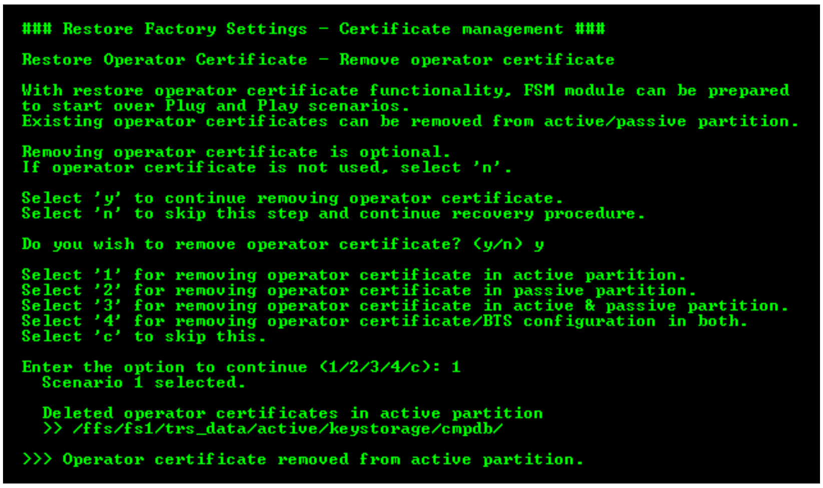
If license keys and Target ID are chosen to be deleted and FZM module is reset in the end of restore procedure, the reset causes an immediate update on timestamp stored at system module.



```
### Restore Factory Settings - Clear BTS Licensing - Logical Target ID ###

BTS Licensing - Logical Target ID for Flexi BTS (RAN1849)
Flexi Multiradio BTS WCDMA
Flexi Lite BTS WCDMA
Flexi Zone WCDMA BTS

The unique Target ID exist in the WBTS consisting system module serial
number and timestamp information <serial number>_<time stamp>
e.g. L6100232744_120551.
If LK and TargetID is deleted, make sure no RF modules are connected to
system module. System module is reset in the end of restore procedure.
The reset causes an immediate update on timestamp stored at system module.

Deleting License Key and Target ID is optional.

Do you wish to delete License Key and TargetID? (y/n) y

>>> License Key and TargetID cleared.
```

3) DELETE OPERATOR CERTIFICATE (optional)

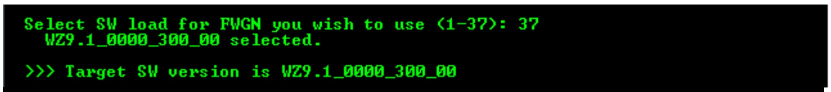
Operator certificates from active and/or passive partition to prepare target unit to start over Plug and Play scenario. Select preferred option to remove operator certificate.



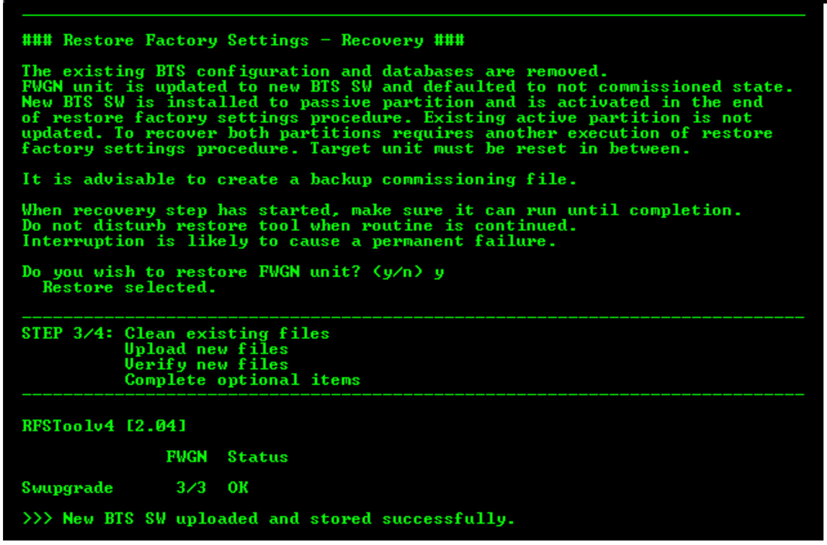
```
### Restore Factory Settings - Certificate management ###

Restore Operator Certificate - Remove operator certificate

With restore operator certificate functionality, FSM module can be prepared
to start over Plug and Play scenarios.
Existing operator certificates can be removed from active/passive partition.

Removing operator certificate is optional.
If operator certificate is not used, select 'n'.

Select 'y' to continue removing operator certificate.
Select 'n' to skip this step and continue recovery procedure.

Do you wish to remove operator certificate? (y/n) y

Select '1' for removing operator certificate in active partition.
Select '2' for removing operator certificate in passive partition.
Select '3' for removing operator certificate in active & passive partition.
Select '4' for removing operator certificate/BTS configuration in both.
Select 'c' to skip this.

Enter the option to continue (1/2/3/4/c): 1
  Scenario 1 selected.

  Deleted operator certificates in active partition
  >> /ffs/fs1/trs_data/active/keystorage/cmpdb/

>>> Operator certificate removed from active partition.
```

4) SELECT SW RELEASE FOR RECOVERY PROCEDURE

Select target SW from list (made of SW loads stored in \BTSSW\).
Confirm to start recovery procedure.



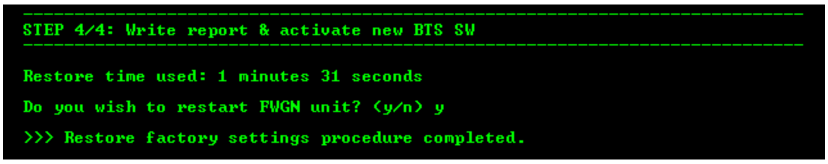
```
Select SW load for FWGN you wish to use (1-37): 37
  WZ9.1_0000_300_00 selected.

>>> Target SW version is WZ9.1_0000_300_00
```



```
------------------------------------------------------------------------------

### Restore Factory Settings - Recovery ###

The existing BTS configuration and databases are removed.
FWGN unit is updated to new BTS SW and defaulted to not commissioned state.
New BTS SW is installed to passive partition and is activated in the end
of restore factory settings procedure. Existing active partition is not
updated. To recover both partitions requires another execution of restore
factory settings procedure. Target unit must be reset in between.

It is advisable to create a backup commissioning file.

When recovery step has started, make sure it can run until completion.
Do not disturb restore tool when routine is continued.
Interruption is likely to cause a permanent failure.

Do you wish to restore FWGN unit? (y/n) y
  Restore selected.

------------------------------------------------------------------------------
STEP 3/4: Clean existing files
          Upload new files
          Verify new files
          Complete optional items
------------------------------------------------------------------------------

RFSToolv4 [2.04]

              FWGN  Status

Swupgrade      3/3  OK

>>> New BTS SW uploaded and stored successfully.
```

5) RESTART FZM MODULE, CLOSE APPLICATION & OBSERVE LOG FILE

FZM module is not automatically restarted to take new SW in use.
Select option to trigger SW activation restart.



```
------------------------------------------------------------------------------
STEP 4/4: Write report & activate new BTS SW
------------------------------------------------------------------------------

Restore time used: 1 minutes 31 seconds

Do you wish to restart FWGN unit? (y/n) y

>>> Restore factory settings procedure completed.
```

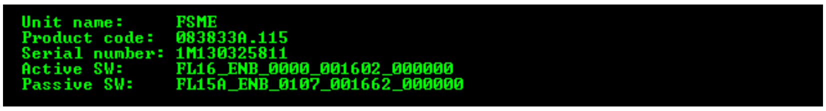
After each execution, a report file in txt format is created that is significant to each system module based on the serial number and current date/time. RFS report file name is specified by the serial number, product code, current date and time (e.g. C:\Temp\RFSToolv4\logs\L6130705629_084792A.101__20140902_143756.txt). RFS report is stored to \logs under restore tool root directory.

8.5 Procedure – preparations FSME/FSMD

If LTE to WCDMA technology change is needed, refer to RFSTool2.

1) DATA COLLECTION FROM FSME

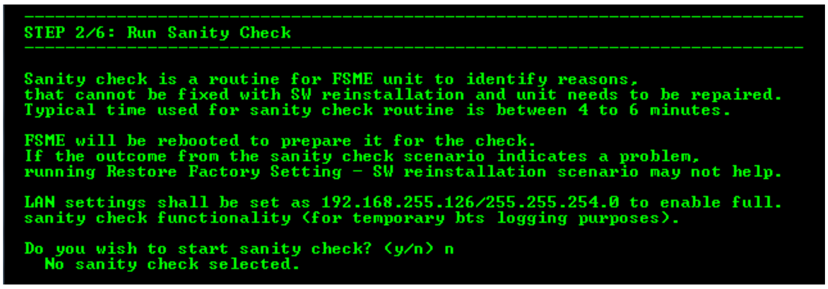
The progress of required connections, unit and SW version information found is displayed.



```
Unit name:     FSME
Product code:  083833A.115
Serial number: 1M130325811
Active SW:     FL16_ENB_0000_001602_000000
Passive SW:    FL15A_ENB_0107_001662_000000
```

2) SANITY CHECK (optional)

For FSME/D/C a scenario called ‘Sanity Check’ (SC) can be optionally executed. SC is a routine which may identify further reasoning why FSM unit is not working properly.
The faults and notifications reported in SC results can indicate for example if one of the FSPC subunits or one of the DSP’s are not responding to SC routine. Is done both in LTE and WCDMA.

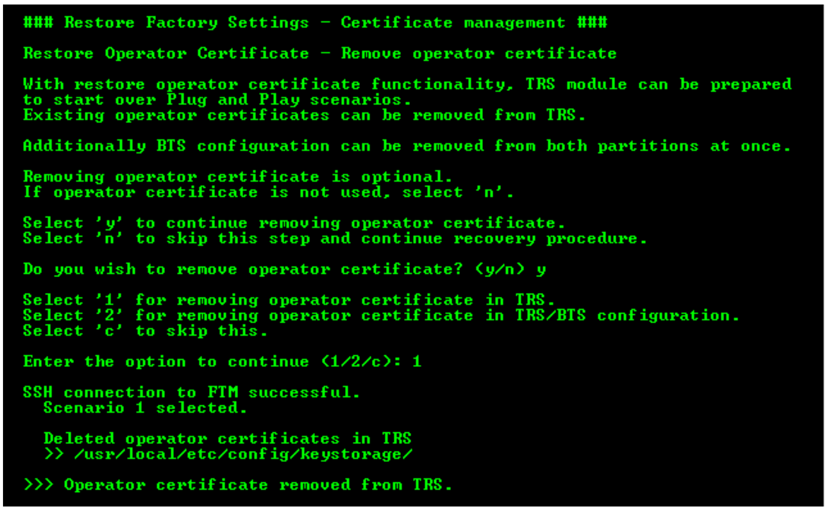


```
-----------------------------------------------------------------------------
STEP 2/6: Run Sanity Check
-----------------------------------------------------------------------------

Sanity check is a routine for FSME unit to identify reasons,
that cannot be fixed with SW reinstallation and unit needs to be repaired.
Typical time used for sanity check routine is between 4 to 6 minutes.

FSME will be rebooted to prepare it for the check.
If the outcome from the sanity check scenario indicates a problem,
running Restore Factory Setting - SW reinstallation scenario may not help.

LAN settings shall be set as 192.168.255.126/255.255.254.0 to enable full.
sanity check functionality (for temporary bts logging purposes).

Do you wish to start sanity check? (y/n) n
  No sanity check selected.
```

After sanity check routine, SW installation can be done to complete restore procedure. If FSM unit still do not function properly after SW update, refer to SC findings (faults/notification) to identify if SC can specify more detailed reasoning.

3) DELETE OPERATOR CERTIFICATE (optional)

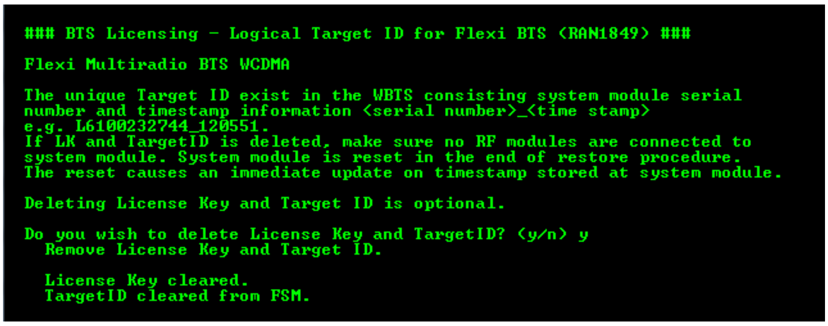
Operator certificates from active and/or passive partition to prepare target unit to start over Plug and Play scenario. Select preferred option to remove operator certificate.



```
### Restore Factory Settings - Certificate management ###

Restore Operator Certificate - Remove operator certificate

With restore operator certificate functionality, TRS module can be prepared
to start over Plug and Play scenarios.
Existing operator certificates can be removed from TRS.

Additionally BTS configuration can be removed from both partitions at once.

Removing operator certificate is optional.
If operator certificate is not used, select 'n'.

Select 'y' to continue removing operator certificate.
Select 'n' to skip this step and continue recovery procedure.

Do you wish to remove operator certificate? (y/n) y

Select '1' for removing operator certificate in TRS.
Select '2' for removing operator certificate in TRS/BTS configuration.
Select 'c' to skip this.

Enter the option to continue (1/2/c): 1

SSH connection to FTM successful.
  Scenario 1 selected.

  Deleted operator certificates in TRS
  >> /usr/local/etc/config/keystorage/

>>> Operator certificate removed from TRS.
```

4) DELETE LICENSE KEY – TARGET ID [WCDMA] (optional)

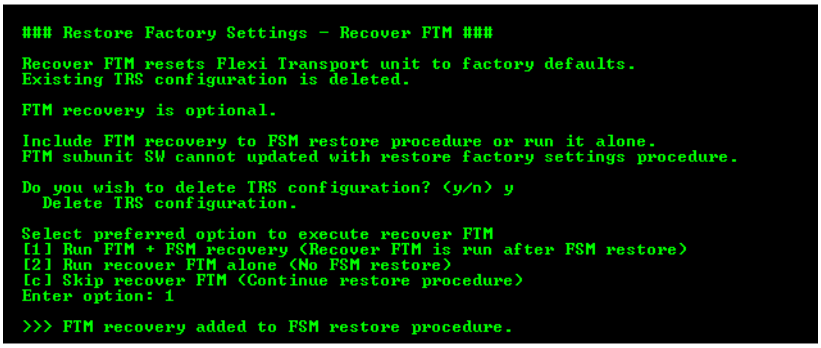
If LK and Target ID is deleted, make sure no RF modules are connected to '
system module. System module is reset in the end of restore procedure. '
The reset causes an immediate update on timestamp stored at system module.'



```
### BTS Licensing - Logical Target ID for Flexi BTS (RAN1849) ###

Flexi Multiradio BTS WCDMA

The unique Target ID exist in the WBTS consisting system module serial
number and timestamp information <serial number>_<time stamp>
e.g. L6100232744_120551.
If LK and TargetID is deleted, make sure no RF modules are connected to
system module. System module is reset in the end of restore procedure.
The reset causes an immediate update on timestamp stored at system module.

Deleting License Key and Target ID is optional.

Do you wish to delete License Key and TargetID? (y/n) y
  Remove License Key and Target ID.

  License Key cleared.
  TargetID cleared from FSM.
```

5) RECOVER FTM (optional)

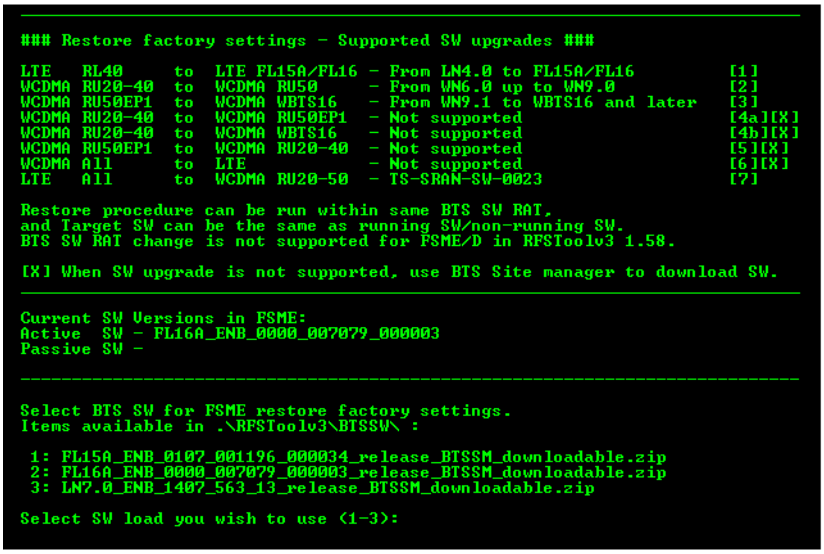
Recover FTM resets Flexi Transport unit to factory defaults. Existing TRS configuration is deleted. Local account password is set to factory default.



```
### Restore Factory Settings - Recover FTM ###

Recover FTM resets Flexi Transport unit to factory defaults.
Existing TRS configuration is deleted.

FTM recovery is optional.

Include FTM recovery to FSM restore procedure or run it alone.
FTM subunit SW cannot updated with restore factory settings procedure.

Do you wish to delete TRS configuration? (y/n) y
  Delete TRS configuration.

Select preferred option to execute recover FTM
[1] Run FTM + FSM recovery (Recover FTM is run after FSM restore)
[2] Run recover FTM alone (No FSM restore)
[c] Skip recover FTM (Continue restore procedure)
Enter option: 1

>>> FTM recovery added to FSM restore procedure.
```

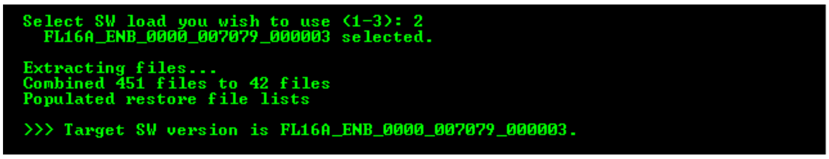
6) SELECT SW RELEASE FOR RECOVERY PROCEDURE

Select target SW from list (made of SW loads stored in \BTSSW\).
Confirm to start recovery procedure.

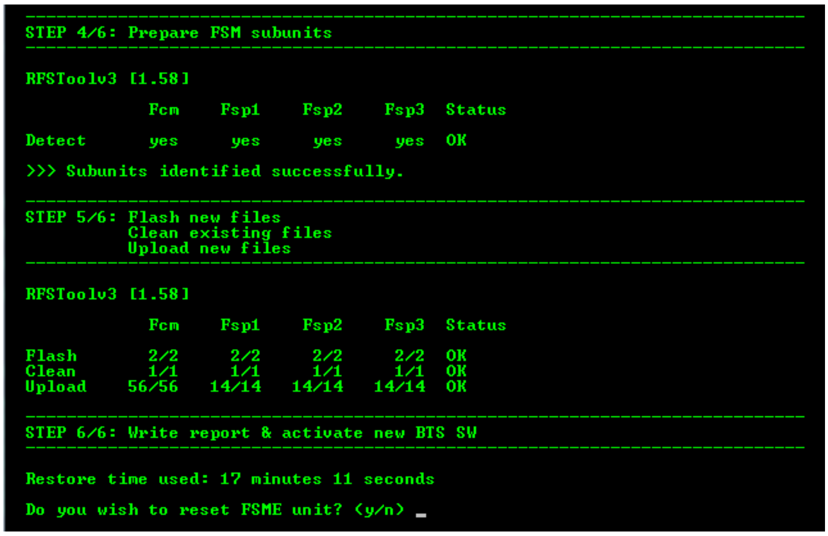


```
### Restore factory settings - Supported SW upgrades ###

LTE   RL40     to  LTE FL15A/FL16 - From LN4.0 to FL15A/FL16        [1]
WCDMA RU20-40  to  WCDMA RU50     - From WN6.0 up to WN9.0          [2]
WCDMA RU50EP1  to  WCDMA WBTS16   - From WN9.1 to WBTS16 and later  [3]
WCDMA RU20-40  to  WCDMA RU50EP1  - Not supported                   [4a][X]
WCDMA RU20-40  to  WCDMA WBTS16   - Not supported                   [4b][X]
WCDMA RU50EP1  to  WCDMA RU20-40  - Not supported                   [5][X]
WCDMA All      to  LTE            - Not supported                   [6][X]
LTE   All      to  WCDMA RU20-50  - TS-SRAN-SW-0023                 [7]

Restore procedure can be run within same BTS SW RAT,
and Target SW can be the same as running SW/non-running SW.
BTS SW RAT change is not supported for FSME/D in RFSToolv3 1.58.

[X] When SW upgrade is not supported, use BTS Site manager to download SW.

Current SW Versions in FSME:
Active  SW - FL16A_ENB_0000_007079_000003
Passive SW -

----------------------------------------------------------------------------

Select BTS SW for FSME restore factory settings.
Items available in .\RFSToolv3\BTSSW\ :

 1: FL15A_ENB_0107_001196_000034_release_BTSSM_downloadable.zip
 2: FL16A_ENB_0000_007079_000003_release_BTSSM_downloadable.zip
 3: LN7.0_ENB_1407_563_13_release_BTSSM_downloadable.zip

Select SW load you wish to use (1-3):
```

LTE SW update example

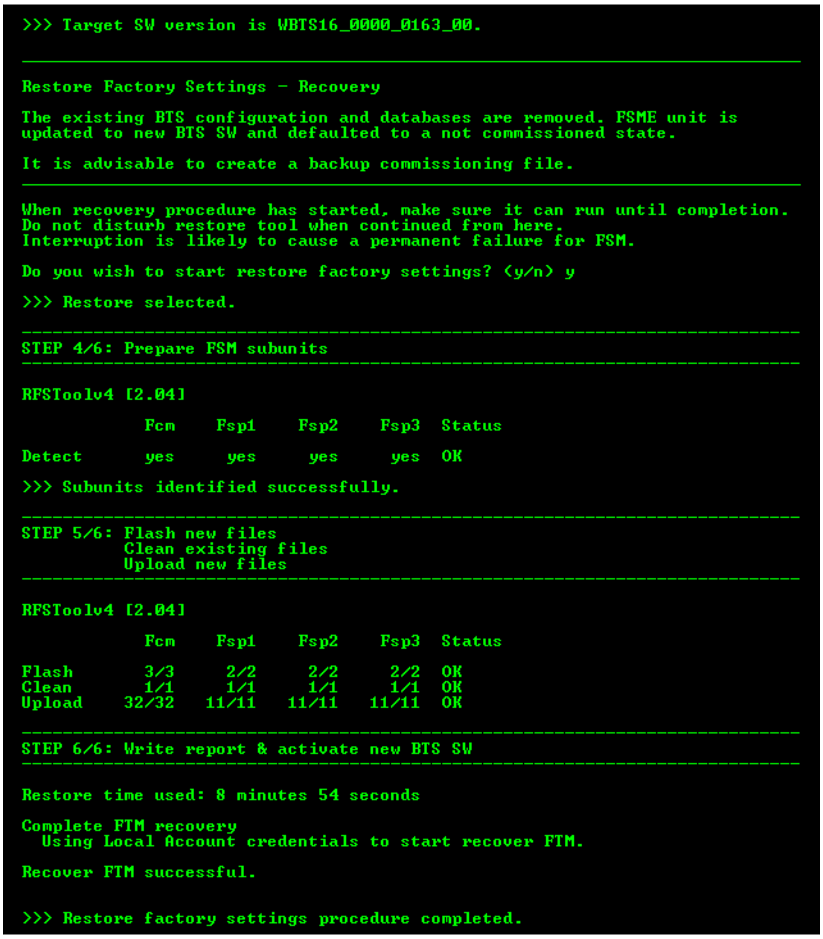


```
Select SW load you wish to use (1-3): 2
  FL16A_ENB_0000_007079_000003 selected.

Extracting files...
Combined 451 files to 42 files
Populated restore file lists

>>> Target SW version is FL16A_ENB_0000_007079_000003.
```



```
----------------------------------------------------------------------------
STEP 4/6: Prepare FSM subunits
----------------------------------------------------------------------------

RFSToolv3 [1.58]

            Fcm    Fsp1    Fsp2    Fsp3  Status

Detect      yes     yes     yes     yes  OK

>>> Subunits identified successfully.

----------------------------------------------------------------------------
STEP 5/6: Flash new files
          Clean existing files
          Upload new files
----------------------------------------------------------------------------

RFSToolv3 [1.58]

            Fcm    Fsp1    Fsp2    Fsp3  Status

Flash       2/2     2/2     2/2     2/2  OK
Clean       1/1     1/1     1/1     1/1  OK
Upload    56/56   14/14   14/14   14/14  OK

----------------------------------------------------------------------------
STEP 6/6: Write report & activate new BTS SW
----------------------------------------------------------------------------

Restore time used: 17 minutes 11 seconds

Do you wish to reset FSME unit? (y/n) _
```

WCDMA SW update example



```
>>> Target SW version is WBTS16_0000_0163_00.

____________________________________________________________________________

Restore Factory Settings - Recovery

The existing BTS configuration and databases are removed. FSME unit is
updated to new BTS SW and defaulted to a not commissioned state.

It is advisable to create a backup commissioning file.
____________________________________________________________________________

When recovery procedure has started, make sure it can run until completion.
Do not disturb restore tool when continued from here.
Interruption is likely to cause a permanent failure for FSM.

Do you wish to start restore factory settings? <y/n> y

>>> Restore selected.

----------------------------------------------------------------------------
STEP 4/6: Prepare FSM subunits
----------------------------------------------------------------------------

RFSToolv4 [2.04]

            Fcm    Fsp1    Fsp2    Fsp3  Status

Detect      yes     yes     yes     yes  OK

>>> Subunits identified successfully.

----------------------------------------------------------------------------
STEP 5/6: Flash new files
          Clean existing files
          Upload new files
----------------------------------------------------------------------------

RFSToolv4 [2.04]

            Fcm    Fsp1    Fsp2    Fsp3  Status

Flash       3/3     2/2     2/2     2/2  OK
Clean       1/1     1/1     1/1     1/1  OK
Upload    32/32   11/11   11/11   11/11  OK

----------------------------------------------------------------------------
STEP 6/6: Write report & activate new BTS SW
----------------------------------------------------------------------------

Restore time used: 8 minutes 54 seconds

Complete FTM recovery
  Using Local Account credentials to start recover FTM.

Recover FTM successful.


>>> Restore factory settings procedure completed.
```

7) RESTART FSM MODULE, CLOSE APPLICATION & OBSERVE LOG FILE

FSM module is not automatically restarted to take new SW in use.
Select option to trigger SW activation restart.

If ‘Recover FTM option 1’ is selected, TRS and FSM are automatically restarted.

After each execution, a report file in txt format is created that is significant to each system module based on the serial number and current date/time. RFS report file name is specified by the serial number, product code, current date and time (e.g. C:\Temp\RFSToolv4\logs\L6130705629_084792A.101__20140902_143756.txt). RFS report is stored to \logs under restore tool root directory.

8.6 SW management

FSM unit is restored to user selected target BTS SW. RFS tool can update SW to interim BTS SW release or directly to target BTS SW release.

Optional sub-units of Flexi Multiradio 10 System Module FSMF

- With FSMF, optional subunits including FTIF and FBBx are updated simultaneously.
- With FSIH, optional subunits including FBIH are updated simultaneously.

  Note: FTIF (Flexi Transport Interface) is different to FTM (Flexi Transport Module). FTIF is an interface card in FSMF to provide more connections. It does not have separate control module as FTM. Therefore, FTIF does not provide similar command line interface functionality as FTM module.

Transmission sub-units of Flexi Multiradio System Module FSME

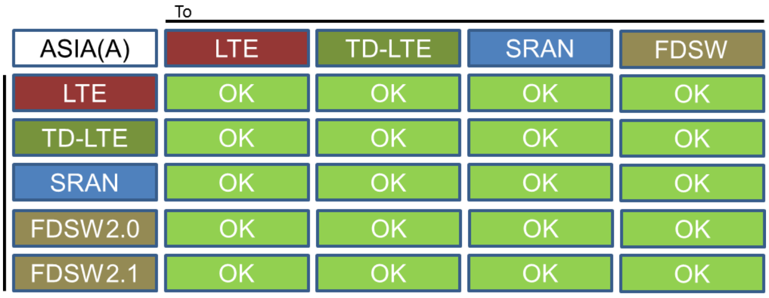
- With FSME/D/C, transmission subunit is not updated. Active TRS configuration can be cleared (also Local account settings are removed).

Extension system modules / RF modules

- No update is done to Extension system module and RF modules in the BTS configuration
- The SW update functionality of restore factory settings makes an update only on FSM.
- Extension system modules shall be treated as standalone FSM units with restore factory settings procedure.

8.6.1 SW compatibility – ASIA/ASIAA

The following figure displays how ASIA/ASIAA SW updates are supported with RFS Tool. All BTS SW releases available in NOLS are supported.



	To			
ASIA(A)	LTE	TD-LTE	SRAN	FDSW
LTE	OK	OK	OK	OK
TD-LTE	OK	OK	OK	OK
SRAN	OK	OK	OK	OK
FDSW2.0	OK	OK	OK	OK
FDSW2.1	OK	OK	OK	OK

8.6.2 SW compatibility - FSMF

The following figure displays how FSMF SW updates are supported with RFS Tool.
All BTS SW releases available in NOLS are supported.

To

FSMF	LTE	WCDMA	TD-LTE	GSM	SRAN	FDSW
LTE	OK	OK	OK	N/A [2]	OK	OK
WCDMA	OK	OK	OK	N/A [2]	OK	OK
TD-LTE	OK	OK	OK	N/A [2]	OK	OK
GSM	OK	OK	OK	N/A [2]	OK	OK
SRAN	OK	OK	OK	N/A [2]	OK	OK
FDSW1.0	N/A [1]	N/A [1]	N/A [1]	N/A [2]	N/A [1]	N/A [1]
FDSW1.1	OK	OK	OK	N/A [2]	OK	OK
FDSW1.3	OK	OK	OK	N/A [2]	OK	OK
FDSW2.0	OK	OK	OK	N/A [3]	OK	OK

1) SW update from FDSW1.0 to WCDMA/LTE/TD-LTE is not possible. Use BTS Site manager.
2) Use 2G BTS Site manager and 2G Target BD formatted SW package to update FSMF from another RAT SW to GSM
3) Utilize RFS tool to update FSMF first to LN7.0 and then with 2G BTS Site manager & 2G Target BD formatted SW package update SW to GF release.

Note: If SW update from other RAT to GSM using BTS Site manager does not work – it is recommended to restore FSM to RL70 level SW first and then SW update from BTS Site manager shall be deployed.

8.6.3 SW compatibility – FSMFA

The following figure displays how FSMFA SW updates are supported with RFS Tool.
All BTS SW releases available in NOLS are supported.

To

FSMFA	LTE	TD-LTE	SRAN	FDSW
LTE	OK	OK	OK	OK
TD-LTE	OK	OK	OK	OK
SRAN	OK	OK	OK	OK
FDSW1.2	OK	OK	OK	OK
FDSW1.4	OK	OK	OK	OK

8.6.4 SW compatibility – FSIH/FQxx/FWxx

All BTS SW releases available in NOLS are supported.

8.6.5 SW compatibility – FSME/FSMD/FSMC

Refer to compatibility table in chapter 2 for supported WCDMA and LTE SW update paths included to restore tool. An approximate time required for RFSToolv4 SW update from 8 to 23 minutes.

Restore tool does not support all possible SW configurations and therefore a certain SW upgrade scenarios cannot be done (Due to chancing operating system in WCDMA technology).

WCDMA RU20-40	to	WCDMA RU50	- From WN6.0 up to WN9.0	
WCDMA RU50EP1	to	WCDMA WBTS16	- From WN9.1 to WBTS16 and later	
WCDMA RU20-40	to	WCDMA RU50EP1	- Not supported	[X]
WCDMA RU20-40	to	WCDMA WBTS16/17	- Not supported	[X]
WCDMA RU50EP1	to	WCDMA RU20-40	- Not supported	[X]
WCDMA All	to	LTE All	- Not supported	[X]
LTE All	to	LTE All	- From LN3.0 to FL16 and later	

[X] When SW update is not supported, use BTS Site manager to download SW.

Restore procedure can be run within same BTS SW RAT and Target SW can be the same as running SW/non-running SW. BTS SW RAT change is not supported for FSME/D.

8.7 Troubleshooting / Q&A

8.7.1 Restore tool in BTS Site manager delivery vs. standalone delivery

There can be different versions available in BTS Site manager delivery vs. what is made available through NOLS and Nokia support. Due to fault correction and improvement/new functionality being added, latest versions to BTS Site manager can come later available.

Applications inside BTS Site manager delivery vs. in NOLS delivery via technical note are different. Therefore, they may not work correctly if not used in dedicated environment surrounded with released supporting files.

8.7.2 Logs – RFS report

After each execution, a report file in txt format is created that is significant to each system module based on the serial number and current date/time. Restore tool report is stored to .\RFSToolv4\logs. The report includes in more detailed level the actions and message scenarios between restore tool and target FSM unit.

RFS report file name is specified by the serial number, product code, current date and time (e.g. L6130705629_084792A.101__20140902_143756.txt).

When unit identification information cannot be retrieved, meaning the access to system module was not available or system module is not able to provide the requested information, the report file does not specify serial number and product code information (e.g. NA_NA__201402808_094948.txt).

After successful recovery, system module has been set to default factory settings. If same problem still exists and BTS cannot reach operational state, system module may have more severe failure that cannot be recovered with recovery tool.

8.7.3 Problems

Before recovery, no ping responses available at 192.168.255.1/.127/.129/.131

If no ping response is available at 192.168.255.1/.127/.129/.131, restore factory settings procedure cannot be executed successfully.

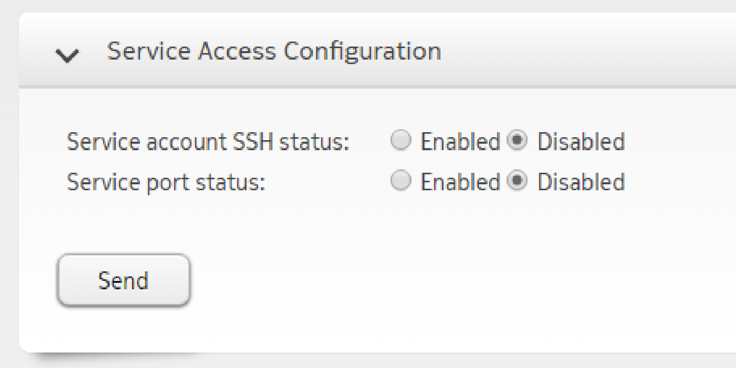
With FSMF if recovery cannot start due failing TCP connections, deploy additional reset to FSMF module by using reset button next EIF1 connector.

After successful recovery, no ping responses available at FSM.

After successful recovery scenario, occasionally ping response at 192.168.255.129 may not be resumed. This may happen when FSM RAT is changed during restore procedure. If LED's of 'FAN' is solid green and 'STATUS' is solid yellow and LED's for optical ports 'RF/EXT1', 'RF/EXT2' and 'RF/EXT3' have solid yellow indicated, additional power cycle is required to regain access to FSM unit.

Restore tool cannot login to SBTS (FSMF).

With enabling service Access configuration, it can help restore tool to gain access and create needed TCP connection to complete restore procedure. In SBTS Site manager, select Monitoring and tests | Service Access Configuration to ease access.



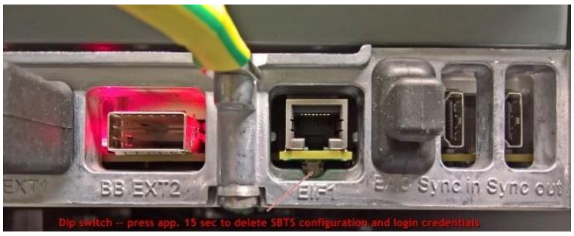
Service Access Configuration

Service account SSH status: ○ Enabled ● Disabled

Service port status: ○ Enabled ● Disabled

Recover SBTS Local account

In case local account has been changed and needs to be recovered (set to defaults), press and hold this dip switch in FSMF for 10 seconds and wait 2 minutes. Then finalize cleaning procedure with additional reset to FSMF (press reset button quickly again. This will delete configuration file as well as Local account login credentials.



Dip switch -- press app. 15 sec to delete SBTS configuration and login credentials

Restore tool cannot login to FSM (FL16A/TL16A)

When FSMF is equipped FL16A/TL16A, to enable successful connections for restore tool, user may have to enable R&D port and SSH services manually from Nokia Transport Module Web Interface. Restore tool version 1.48 and later shall perform this automatically.

1) Open https:/192.168.255.129/
2) Enter username and password, default value: 'Nemuadmin/nemuuser'.
3) Select 'R&D Port Service' on the left hand side panel
   and select 'Enable R&D port Service' to allow test port usage.
4) Select 'SSH Service' on the left hand side panel
   and select 'Enable SSH' to allow secured connections.
5) Try again to run restore procedure.

Java errors displayed and recovery routine cannot complete

Check that ChangeEthernetSecurityTool4.zip (62MB file) is located in restore tool root directory. Version 1.45 and later can be used only with ChangeEthernetSecurityTool4.
ChangeEthernetSecurityTool2 does not work with versions < 1.36.
ChangeEthernetSecurityTool3 does not work with versions < 1.42.
ChangeEthernetSecurityTool4 does not work with versions < 1.45.

Note: The above is not applicable when using restore tool delivered through BTS Site manager.

Application continues without input from user

The input from user is saved to cache and is fed to RFS tool application. If by accident more input were entered, RFS will continue to work on the scenario (if input is acceptable for the step). This can lead to situations with undesired completion.

New SW does not activate, instead a SW fallback is detected

Perform SW update to FDSW first and then to target SW.

All other errors

Restore tool application is guiding what needs to be done to be successful in restore factory settings procedure. In case of a recovery procedure is not fully completed or it is discontinued, retry to run recovery procedure.

9. REFERENCES

TS-SRAN-HW-0080, System Module recovery with Restore Factory Settings
TS-SRAN-HW-0108, FDSW as a factory load for System Module