WebEM User Guide

DN192692940
Issue 07B
Approval Date 2019-05-30

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 document is Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of 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.

Table of Contents

This document has 97 pages

List of Figures

List of Tables

Summary of changes

A list of changes between document issues. You can navigate through the respective changed topics.

In this summary of changes:

This document is common for all Radio Access Technologies (RAT). You can find here information about solutions that are not available or supported in a specific SW release or RAT. *Table: RAT releases covered by the document* lists all SW releases covered by the content of this document. For features supported in your SW release, see the respective feature documentation in the system library.

Table 1 RAT releases covered by the document

Radio Access Technology (RAT)	Release
SRAN	SRAN 19, SRAN 18A, SRAN 18 SP, SRAN 18, SRAN 17A
Long Term Evolution	LTE 19

Changes between issues 07A (2019-03-20, SRAN/LTE 19) and 07B (2019-05-30, SRAN/LTE 19)

Calibrate EPIMC FHS

- The topic has been added.

BTS Log Level

- The topic has been added.

Frequently asked questions about WebEM

- The topic has been added.

Changes between issues 07 (2019-02-22, SRAN/LTE 19) and 07A (2019-03-20, SRAN/LTE 19)

Options menu

- Note to section **Settings** has been added

Validation errors (Definition, Relation, Hardware)

- The note has been added.

Recommended way of refreshing the running WebEM session

- The task has been added.

Changes between issues 06A (2018-12-04, SRAN 18A) and 07 (2019-02-22, SRAN/LTE 19)

Top Menu

- Information on the **Download application** button has been added.

User Account Management

- Information on the amount of open sessions has been added.

Alarms in WebEM

- Section Fault Toggling History has been added.

Ethernet Port Mirroring

- New topic has been added.

Ethernet Link OAM

- New topic has been added.

Ethernet Service OAM

- The topic has been added.

Routing Policies

- Note has been added.

PMTU Discovery

- The topic has been added.

PDH Loopback

- The topic has been added.

Calibrate EPIMC FHS

- The topic has been added.

Viewing RF monitoring results

- The topis has been added.

1 Introduction to WebEM

WebEM overview, requirements and functionality

WebEM overview

WebEM (Web Element Manager) is a web-based application for maintaining and commissioning a BTS. WebEM can be used in both online (direct connection to the BTS) and offline mode (saved WebEM application) for configuration creation, modification and troubleshooting purposes.

Using WebEM does not interfere with the usage of other element managers, although it is not recommended to have more than one type of element manager type connected to the site at the same time.

WebEM is used starting with the SRAN 17A and LTE 19 releases.

Requirements

To connect to the BTS, type in the BTS management plane IP address (or LMP IP address in case of a local connection), using one of the supported Internet browsers:

- Chrome (recommended), three latest major versions compared to the release date
- Mozilla Firefox, three latest major versions compared to the release date

WebEM can be launched from any PC that can run Chrome or Firefox browser, but for better performance, the following specification is required:

- The minimum screen resolution: 1366x768 pixels (1920x1080 is recommended)
- CPU: 2 GHz 32-bit (x86) or 64-bit (x64)
- RAM: 4 GB

Note: Depending on the browser type or version, loading WebEM from the browser cache may cause the application not to load successfully. In such a case, it is required to either clear the browser cache or refresh the page disregarding the cache (Ctrl+F5).

Functionality

As long as WebEM remains launched and connected to the BTS, the updates are collected constantly with WebEM defined period.

WebEM introduces a new type of file, the Info Model Snapshot file (IMS2). The Info Model Snapshot contains the full BTS runtime data for a certain period of time. IMS2 files can be saved manually from WebEM, or can be automatically retrieved by WebEM when a BTS snapshot is collected.

The save location of files downloaded from WebEM (for example SCF, IMS2 or snapshot files) depends on the browser settings.

Main differences between BTS Site Manager and WebEM

Table 2 Main differences between the BTSSM and WebEM

BTS Site Manager	Web Element Manager
Application that needs to be downloaded and installed on PC	Web browser tool hosted on BTS
Each BTS software version requires the dedicated BTSSM	Upgrades together with the BTS
Supports only Windows and Linux OS	Operating System independent
Requires Java Runtime Enviroment	No need to install Java Runtime Enviroment
Each product requires dedicated BTSSM	Product independent (LTE, SRAN)
Only one read/write session is supported	Up to ten read/write sessions are supported

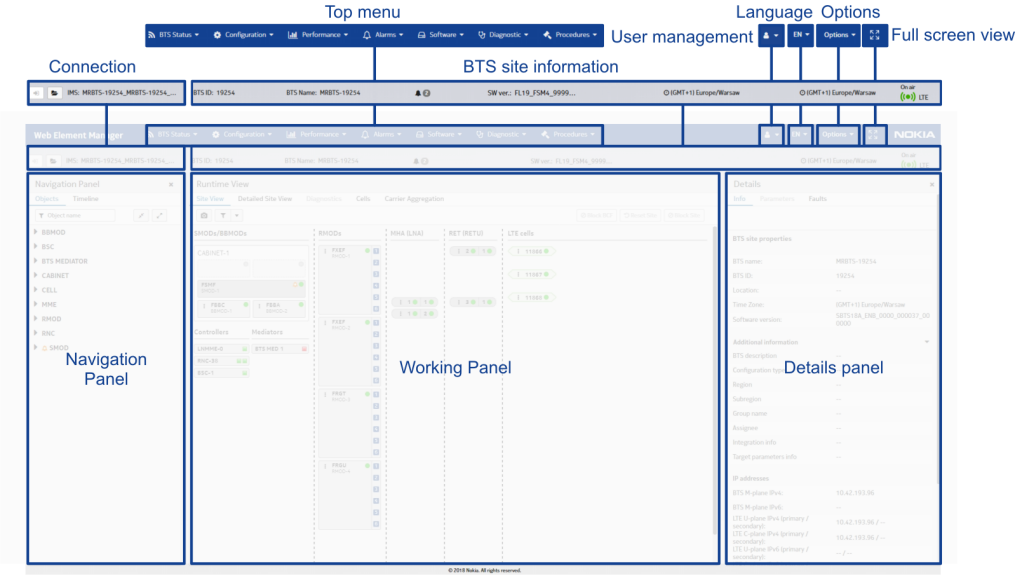
New functionalities introduced by WebEM that were not included in BTSSM:

- New views showing site configuration
  - Site view
  - Detailed Site View
  - Cell View
- New commissioning wizard and parameter editor
- Performance Management
- Alarm Management
- Software Management
- BTS diagnostics
- Timline view

2 WebEM user interface

The WebEM user interface can be divided into the following areas: Connection, BTS site information, Top menu, User management, Language, Options, Navigation Panel, Working Panel and Details Panel.

Figure 1 WebEM user interface overview



Top menu

Main navigation tool of the WebEM application. It allows switching between different views of the working pane. For more information, see: Top menu.

User management

It displays details on the current session and allows the user to log out and open User Account Management.

Language

Language changing is not supported. Only the English version is available.

Options

it contains the following tabs:

- Settings
- Session list
- Operations history
- Download help
- Download application logs
- About
- Download application

For more information, see: Options menu.

Toggle full screen mode

It enables the user to switch on and off full screen mode.

BTS site information

It displays real-time information on the BTS, such as: BTS ID, BTS name, total number of alarms, BTS software version, BTS time zone, technologies configured on the site along with their status. For more information, see: Site Status bar.

Connection

It allows the user to connect to and disconnect from the BTS using the button, open saved IMS2 or snapshot files using the button, and see the actual status of the BTS connection.

Navigation Panel

It lists the timeline information on the BTS state in time as well as objects or errors, depending on the actual view in the working panel. For more information, see: Navigation Panel.

Working Panel

This is the main WebEM working area. For more information, see: Working panel.

Details Panel

It displays details on items selected in the working panel. For more information, see: Details panel.

2.1 Top Menu

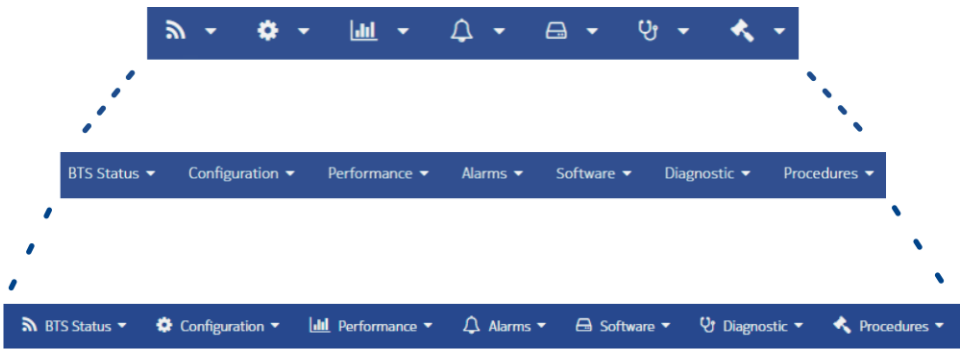
The top menu is the main navigation tool of the WebEM application, allowing the user to switch between different views, change application settings, open user management options or see information on the current WebEM application version.

Top menu

The top menu is the main navigation tool of the WebEM application, allowing the user to switch between different views of the working panel. Clicking on the menu item displays the structured menu of the topic. Clicking on the tab from the structured menu navigates to the selected view.

Top menu layout changes from icons to text depending on the browser window size.

Figure 2 Top menu layout depending on the window size



2.2 Options menu

Description of the options menu.

The **Options** button opens a drop-down list containing the following tabs: **Settings**, **Sessions list**, **Operations history**, **Download help**, **Download application logs**, **About** and **Download application**.

Settings

In the **Settings** window, the user can define the idle screen lock time and disable warnings about unsupported browsers or validation errors in Commissioning Wizard.

Note: The maximum allowed value of the **Lock screen when idle for(min)** parameter is defined by the **WebEM session logout timer** parameter.

To configure **WebEM session logout timer** go to **Configuration ► Configuration Management ► Commissioning Wizard ► Steps ► Security ► User Account Management** .

Session list

The **Session list** menu item displays a table with information about sessions (profile, connection security, session type, IP address, session ID). Note that there is a limit for open sessions - regardless of the user type, up to ten sessions may be open. There are the following session types:

- EM - connection to the BTS through WebEM.
- NMS - connection to the BTS through NetAct.

Operations history

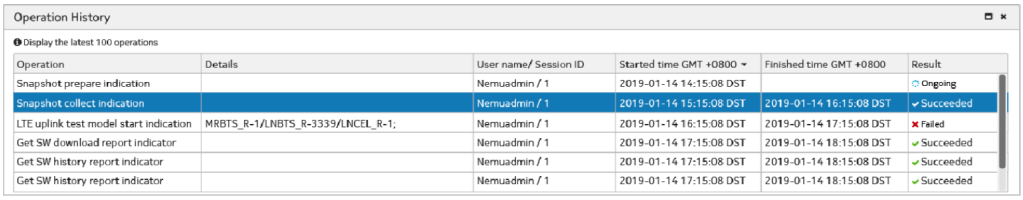
The **Operations history** menu item opens an additional panel with information on executed operations with their statuses. WebEM tracks and displays the user activity that occurred during a single WebEM session.

Operations triggered in the background by WebEM functionalities are also listed in the **Operations history** although they were not triggered by the user.

Operation history panel contains the following information:

- Operation - type of the operation that was performed
- Status - following operation statuses are available:
  - Finished
  - Failed
  - Rejected
  - Ongoing
  - Unknown
- Started - time when the operation has started
- Finished - time when the operation has finished
- Status details - additional information provided by certain operations

Figure 3 Operations history



Download help

The **Download help** option allows the user to download a help file in PDF format.

Download application logs

The **Download application logs** option allows the user to download a help file in PDF format.

Note: If WebEM is running in offline mode (without connection to the BTS) it is not possible to download logs and the Help file.

The **About** option displays main information about the WebEM application:

- Full name
- Version
- Supported browser version
- Build

Download application

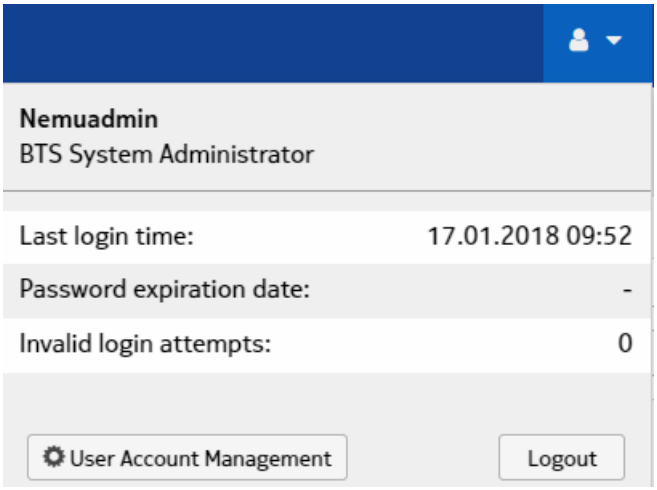
The **Download application** button triggers the download of the offline WebEM version.

2.3 User Account Management

WebEM User Management allows the user to create new or modify existing accounts.

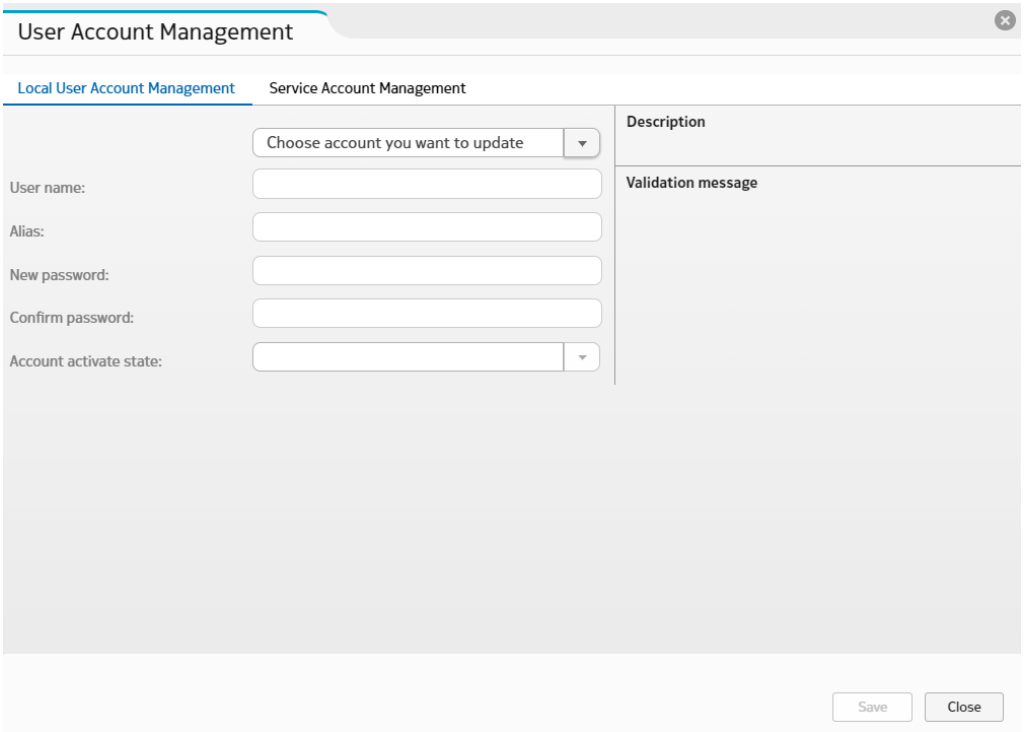
Access to **User Account Management** view: **Top menu ► Username icon ► User Account Management**

Figure 4 Access to User Account Management view



Local User Account Management

Figure 5 Local User Account Management view



Four types of user roles are available in WebEM:

- *BTS System Administrator* - a user who is allowed to update passwords, account active state and aliases for all the other users, as well as update the username (not alias) and password for his own account.
- *BTS Security Administrator* - a user who is allowed to update passwords, account active state and aliases for all users except the BTS System Administrator.
- *BTS Application Administrator* - a user who is allowed to update the password and alias for his own account only.

- *BTS Read - Only* - a user who is allowed to update the password and alias for his own account only. This user also has limitations in performing some types of actions.

Depending on the user type, the following fields are available when editing user accounts:

- **User role**: currently selected user role.
- **User name**: editable only for *BTS System Administrator*.
- **Alias**: not a mandatory field, rules for creating aliases are displayed when the user enters the input field.
- **New password**: rules for creating passwords are displayed if this field is active.
- **Confirm password**
- **Account activate state**: used to define whether the selected user role is active or not.

There are always four accounts available in the BTS (one per role). Local accounts can be set as active.

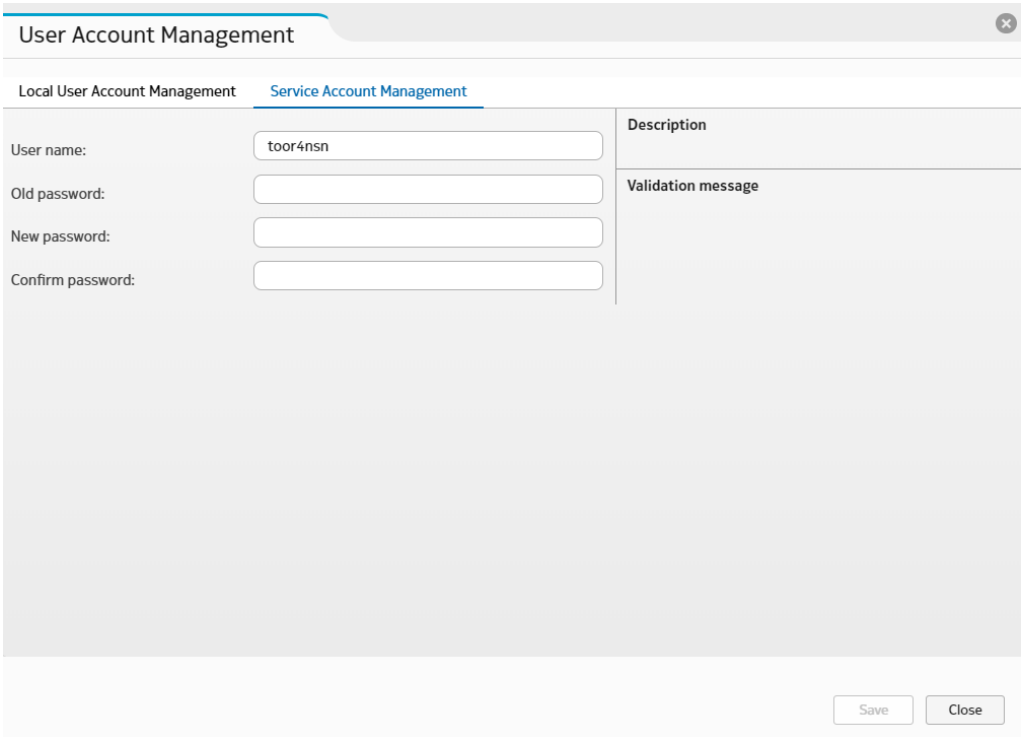
According to the **User role** field displays username as:

- Nemuadmin for *BTS System Administrator*
- BTSSecurity for *BTS Security Administrator*
- BTSApplication for *BTS Application Administrator*
- BTSRead for *BTS Read - Only*

The **Save** button saves any changes made.

Service Account Management

Figure 6 Service Account Management view



Service accounts are used by the technical support personnel in response to service requests made by the operator. Remote or local service access to the BTS is done over the Secure Shell (SSH) protocol, using credential-based authentication (username and password).

- **User name**: mandatory field; user name of the service account for which the password is to be changed.
- **Old password**: mandatory field; the old password must by typed in order to change the existing one; the rules for creating a password are displayed if this field is active.
- **New password**: mandatory field; the new password must be typed in order to change the existing one.
- **Confirm password**

When changing the password, all SSH sessions must be closed.

The **Save** button saves any changes made.

Up to ten sessions can be established in WebEM, all of them with writing rights.

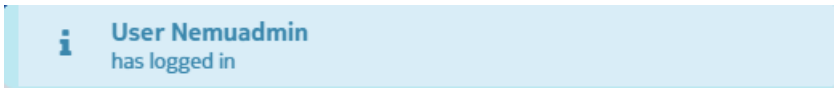
2.4 Notifications in WebEM

Notifications appear in the top-right corner and inform about errors, another user logging in or out, as well as user action status..

Notifications appear in the top-right corner and inform about:

- Another user logged in or out - this type of notification has a blue background and contains the username of the user that has logged in or out.

  Figure 7 Example of notification informing about another user logged in or out

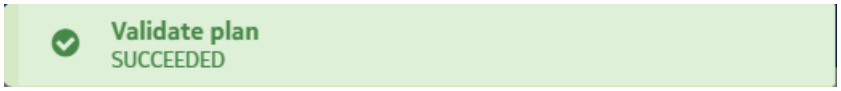
- Errors - this type of notification has a red background.

  Figure 8 Example of notification informing about errors

- User action status (started, accepted or succeeded) - this type of notification has a green background. Types of user actions:
  - block/unblock radio, site
  - lock/unlock cells
  - reset site
  - software activation, rollback
  - test triggered

  Figure 9 Example of user action status notification

2.5 Site Status bar

Shows BTS site and connection status.

The **Site Status** bar is located between the top menu and the working panel.

The connect icon is used to establish or close the connection with the BTS. The open icon is used to load the IMS2 or snapshot file to see the saved data. the file name is displayed next to the icon when it is loaded. Once the IMS2 file is loaded, WebEM is disconnected from the BTS. The message `Connected to BTS` is displayed when WebEM is connected to the BTS.

The **Site Status** bar shows the following:

- BTS ID.
- Site name.
- Number of active alarms.
- Active software version.
- Time zone.
- Configured technologies (GSM, WCDMA, LTE) and their status. The reset button is used to reset a specific technology (available only for WCDMA and LTE).

Resetting a technology causes the reset of the cells and carriers for that technology. It has no impact on the system modules and the rest of the technologies, which continue to provide services.

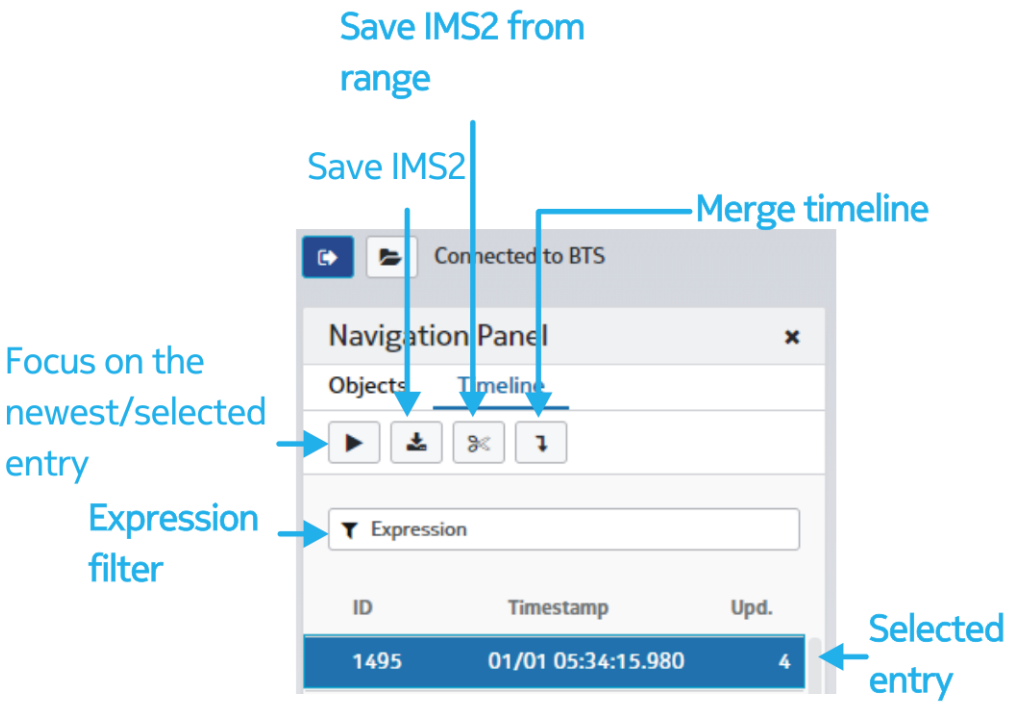
2.6 Navigation Panel

*Located on the left side of the tool, interchangeable between **Timeline**, **Objects** and **Steps** views, depending on which of them are available.*

Navigation panel is located on the left side of the tool. Using the icon hides the panel, while the icon displays it again. Depending on the working panel view, the navigation panel contains three interchangeable tabs: **Timeline**, **Objects**, and **Steps**.

Timeline

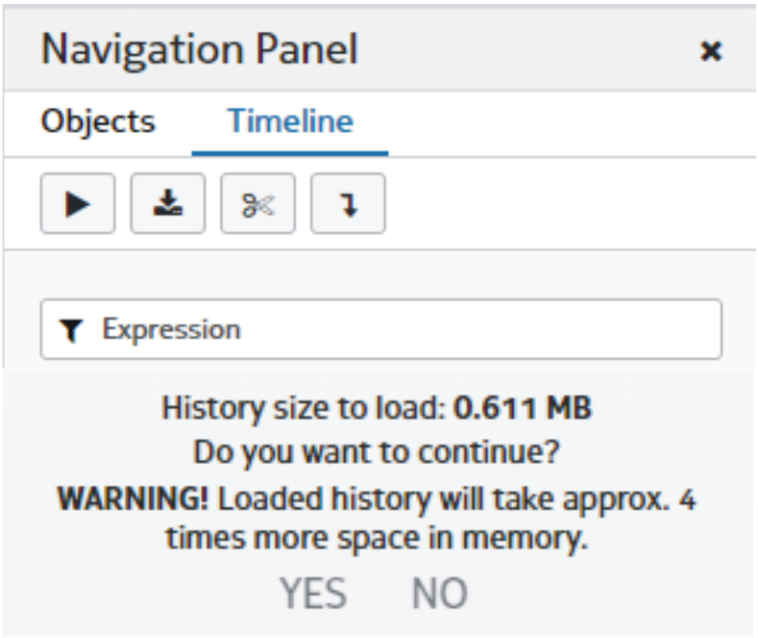
Figure 10 WebEM Timeline tab



The **Timeline** tab lists updates received from the BTS site. It also allows the user to select and display data for a specific time frame. Each timestamp includes detailed information about the BTS state at that certain point in time. Timestamps are displayed in the BTS timezone. As long as the connection between WebEM and the BTS is established, the **Timeline** list is updated with new entries, which can be saved to Info Model Snapshot (IMS2) file at any time. In offline mode, when the IMS2 file is loaded, the list contains all available (saved) entries.

It is possible to load a list of changes that occurred before the connection to the BTS. The history load option appears after the first connection to the BTS, but only when the BTS is synchronized. Clicking the **Yes** button starts the history load process.

Figure 11 History load option



If a timestamp is marked in red, it indicates that a fault occurred during a given period of time. A timestamp in which the alarm ceases to exist is also marked in red. When a BTS is reset, the timestamp contains the label [RST].

Buttons located at the top of the **Timeline** panel allow to:

- **Focus on the newest entry** - focuses on the most actual state (only while connected to the BTS).
- **Save IMS2**
- **Save IMS2 from range**
- **Merge timeline** - allows to merge all visible entries into a single one.

It is possible to filter the visible timestamps based on the affected object names, by using the **Expression filter** located at the top of the **Navigation Panel**.

Selecting a timestamp displays the BTS state from that time stamp.

Changing the view, for example by using either the top menu or tabs, does not affect the items displayed in the **Timeline** tab.

Objects

The **Objects** tab is active for different views. Depending on the view, the **Object** tab shows:

- An object list of the site elements: hardware and cells. An object selected from the list is highlighted in the working panel. Filtering objects is possible by using the **Object name** text field in the navigation panel.
- The configuration plan in a tree format. It is possible to see multiple configuration plans at a time, and the one that is currently used is presented in the designated section **Current BTS configuration**. The **Load SCF** button (located in the working

panel) allows the user to load a configuration from a previously prepared SCF. Newly loaded configurations are added at the bottom, are available locally and are visible in the **Planned BTS configuration** section.

- A list of configuration plans. An object selected from the list is highlighted in the working panel, along with detailed information about the configuration.
- A list of objects with alarms assigned to them, while in the **Alarms** view.
- A list of counters and measurements in **Performance Management** view.

Filtering objects is possible by using the **Object name** search field.

Active and loaded configurations can be modified freely, while changes to the BTS take effect only after using the **Activate Plan** option in the **Parameter Editor** view.

Selecting an object while in Parameter Editor view shows the parameters associated with that object.

Selecting an object while in Definition errors view shows Skipped parameters, Structure errors, Definition errors and Missing object.

Options available in the **Object** view:

- Adding a new configuration plan + (only while viewing configurations).
- Collapsing all objects 
- Expanding all objects 
- Export filter  (only while viewing the **Performance Management** tab)
- Import filter  (only while viewing the **Performance Management** tab)
- Clear all selections  (only while viewing the **Performance Management** tab)

Options available for the selected object (while viewing configurations):

- Adding an object (if available): +
- Removing an object (if available): 
- Undoing any changes made in the runtime configuration (adding or removing objects): 

While in **Configuration Management**, use the **Save BTS Configuration** button to save the configuration on a local drive (available only for the whole configuration).

Figure 12 Objects tab in Runtime View

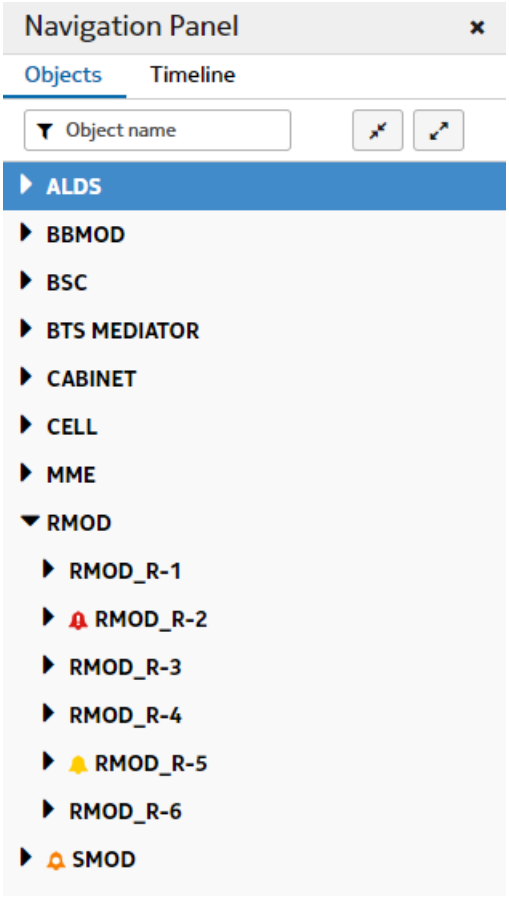
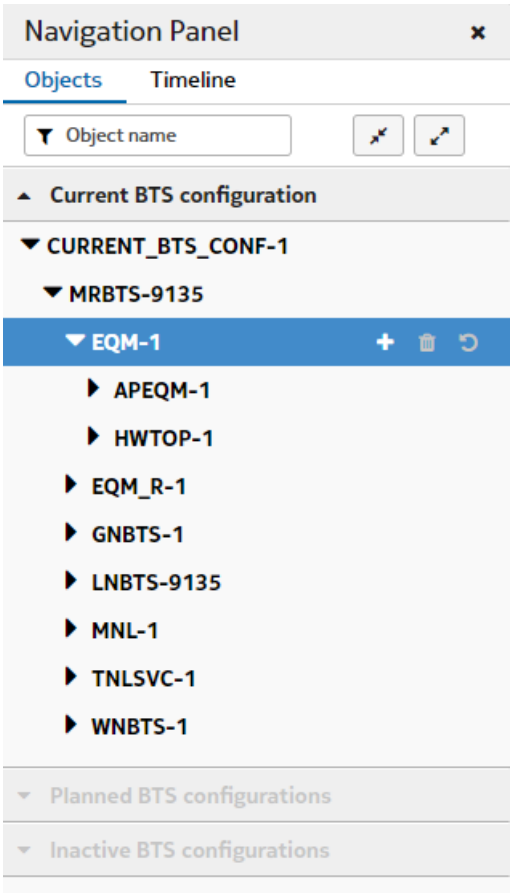


Figure 13 Objects tab in Parameter Editor view



Steps

The **Steps** tab appears only when viewing the **Commissioning Wizard** tab. It shows the configuration plan in a tree format. Clicking on any object opens the **Configuration Wizard** modal view.

2.7 Details panel

***Details** panel description.*

Details panel is located on the right side of the tool. To open **Details** panel click on the ≡ icon.

Details panel displays detailed information on items selected in the **Working** panel. Items displayed in the **Details** view vary depending on the selected item. **Details** panel may contain several tabs.

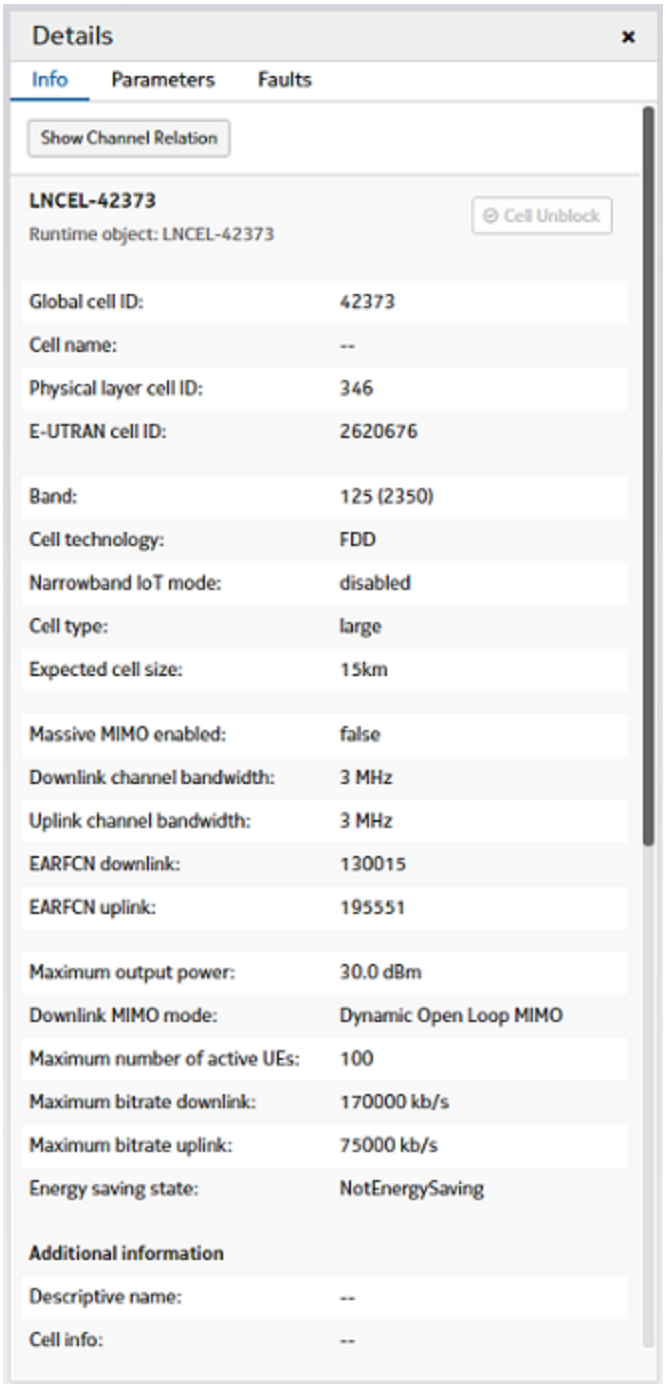
Example of items displayed in **Details** view:

- **Block**/**Unblock**, **Reset**, **Remove** buttons, available when radio module is selected in the **Site Runtime View** or **Cells** view.
- **Cell block**/**Cell unblock**, available when cell is selected in the **Site Runtime View**.

- **Show physical cabinet** button, available when a cabinet is selected in the **Site Runtime View**.
- **Show channel relation** button, available when system module, radio module, extension module, cell and channel are selected in the **Site Runtime View**.
- **Reset** button, available when GNSS module is selected in the **Site Runtime View**.
- Detailed information about an **Alarm** is displayed for all **Alarm Management** views.
- List of active faults assigned to a selected module or cell.
- Related parameters along with their values for the selected object.
- Detailed information on any parameter selected in **Parameter Editor**.
- Detailed information on counters selected in the **Performance Management** view.

Details panel can be hidden by using the hide icon , and shown again by using the details button .

Figure 14 Example of **Details** panel in **Detailed Site View**



2.8 Working panel

Working panel description

Working panel is the main WebEM working area. Available functionalities in the working panel depend on the view. Detailed descriptions of those functionalities are presented in their respective sections:

- BTS Status tab
- Configuration tab
- Performance tab
- Alarms in WebEM
- Software Management tab
- Diagnostic tab
- Procedures tab

3 BTS Status tab

The BTS Status main menu item provides a set of views with options and functionalities that allow the user to view site and configuration details.

3.1 Site Runtime View tab

This view shows the layout and related information.

Site Runtime View consists of the following tabs:

- **Site View** presents a simplified, graphical representation of all site units, active alarms and unit statuses. It allows the user to perform basic operations, like radio module reset or cell unblock.
- **Detailed Site View** presents a detailed, graphical representation of all site units, including links among them, active alarms and unit statuses.
- **Diagnostics** contains a set of tests available only for the transport unit.
- **Cells** lists the cells currently configured on the site.
- **Carrier Aggregation** displays the BTS cells WebEM is connected to as well as cells from other BTSs that are configured as support cells.

Note: WebEM must be refreshed after every BTS power reset in order to update its runtime view.

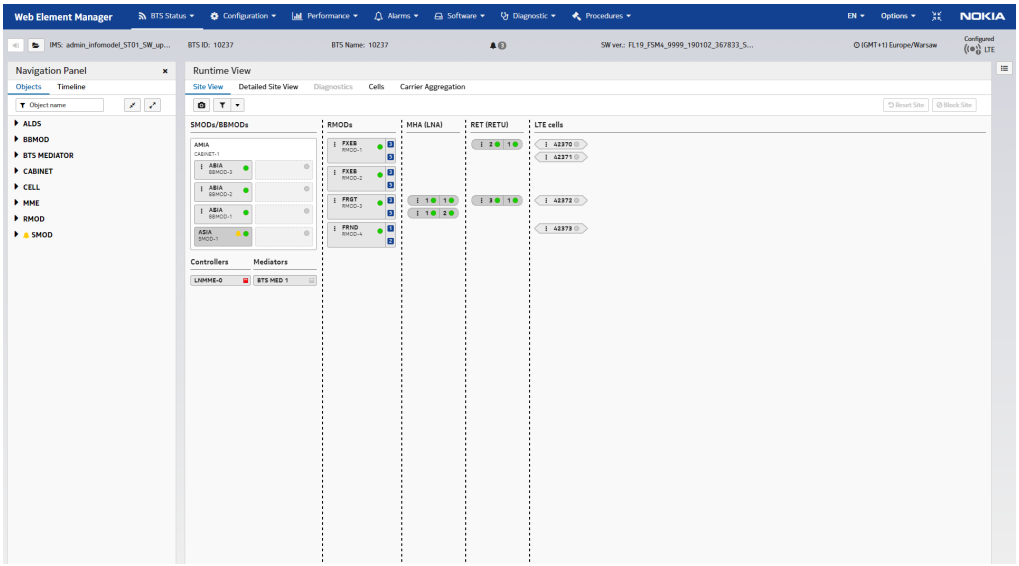
3.1.1 Site View

This view shows the layout and related information.

Access to **Site View** view: **Top Menu ► BTS Status ► Site Runtime View ► Site View**

Site View shows hardware available on the site and configured cells.

Figure 15 Site View



Elements showed in **Site View** can by filtered by:

Hardware

- **Show all**
- **SMODs/BBMODs**
- **External SMODs**
- **BTS Mediators**
- **BTS Contorollers**
- **Fronthaul switches**
- **MHAs/LNAs**
- **RETs/RETUs**
- **RAEs/RAEUs**

Radio ports

- **Show all ports**
- **Show only used ports**

In the **Site View**, some alarms can appear. If an alarm occurs in a particular unit, it is indicated by the alarm icon (the color of the icon represents the severity of the alarm). In case of multiple alarms, the alarm icon on a particular unit indicates only the highest severity, although there may be other alarms. To see the list of alarms for a unit, go to the **Details** panel and open a **Faults** tab. To see even more details about an alarm, use the icon to go to the **Alarm Management** view. The list of alarms is also visible on a tooltip for that alarm.

The **Export as image** icon allows the user to save the site view in PNG format.

In configurations with two FSMF system modules, the modules are displayed in two separate cabinets, due to the physical placement of the modules. In configurations with two ASIA or ASIAA system modules, the modules are displayed in one cabinet.

Selecting any of the elements allows the user to see their details such as basic information (state, name, and so on), and related parameters and faults, when the **Details** panel is expanded. When applicable, some items can be reset, blocked or unblocked using the appropriate buttons from the **Details** panel.

At the top of the view there are site action options, used to block the BCF, reset the site or block and unblock the site. Note that the unblock site function causes the entire BTS to reset.

Figure 16 Site action options

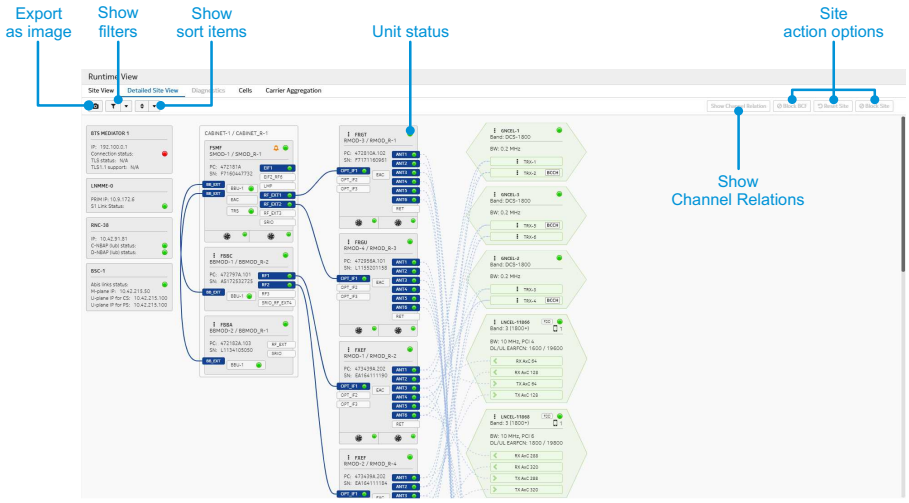
3.1.2 Detailed Site View

> *This view shows the layout and related information.*

Access to **Detailed Site View** view: **Top Menu ► BTS Status ► Site Runtime View ► Detailed Site View**

Detailed Site View shows the hardware available on the site and configured cells, as well as physical and logical links between them (including used ports).

Figure 17 **Detailed Site View**



Connections between site elements and Antenna Line Devices (ALDs) can be filtered from the upper menu. Note that the displayed fiber lengths might differ from the actual lengths.

Available filters:

- **Cell carriers**:
  - **Show cells carriers**
- **ALDs**:
  - **Show all**
  - **Show MHAs**
  - **Show RETs**
  - **Show RAEs**
- **ALD links**:
  - **Show all**
  - **Show configuration links**
  - **Show data links**
  - **Show DC links**
  - **Show RET unit associations**

All elements can also be sorted. **FHSs**, **RMODs** and **ALDs** can be sorted by:

- **Configuration ID**
- **Product name**
- **State**

ALDs can be also sorted by HW type.

Cells can be sorted by:

- **Configuration ID**
- **Band**
- **State**

In the **Detailed Site View**, some alarms can appear. If an alarm occurs in a particular unit, it will be indicated by the alarm icon (the color of the icon represents the severity of the alarm).In case of multiple alarms, the alarm icon on a particular unit indicates only the highest severity, although there may be other alarms. To see the list of alarms for that unit, go to the **Details** panel and open the **Faults** tab. To see even more details about the alarm, use the icon to go to the **Alarm Management** view. A list of alarms is also visible on a tooltip for that alarm.

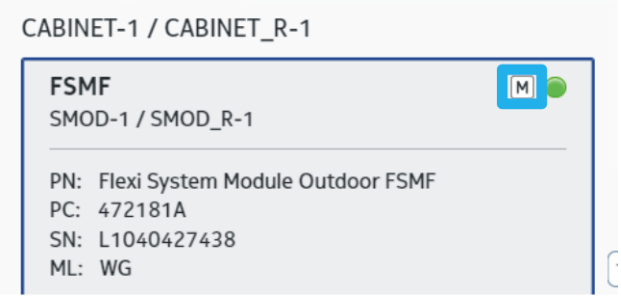
The **Export as image** icon allows the user to save the site view in PNG format.

Selecting the cabinet allows the user to see its details such as basic information (state, name, and so on), and related parameters and faults, when the **Details** panel is expanded. The **Show physical cabinet** button opens a pop-up view displaying the hardware available in the cabinet (including hardware names and port names). Clicking anywhere outside the pop-up window closes it.

In configurations with two FSMF system modules, the modules are displayed in two separate cabinets, due to the physical placement of the modules. In configurations with two ASIA or ASIAA system modules, the modules are displayed in one cabinet.

The master module is marked by the **M** icon.

Figure 18 System module marked as master



Selecting any of the modules, physical connectors, antenna connectors, cells or carriers, allows the user to see their details such as basic information (state, name, and so on), and related parameters and faults, when the **Details** panel is expanded. The **Show Channel Relation** button highlights links and other objects connected to a selected object. If a channel is selected, all the hardware through which data is routed, or elements creating that channel are highlighted. If the selected object is a unit, the button shows the relation between all channels creating or routing data to or from it. If a cell is selected, the button shows the channel relation for this cell.

The **Diagnostics** button opens the diagnostics for the selected transport unit. When applicable, units, cells or GSM TRXs can be reset, blocked or unblocked using the appropriate buttons from the **Details** panel. The icon informs about ongoing procedures for objects. A list of procedures is on a tooltip of this icon. A blocked object is indicated by the icon.

At the top of the view there are site action options, used to block the BCF, reset the site or block and unblock the site. Note that the unblock site function causes the entire BTS to reset.

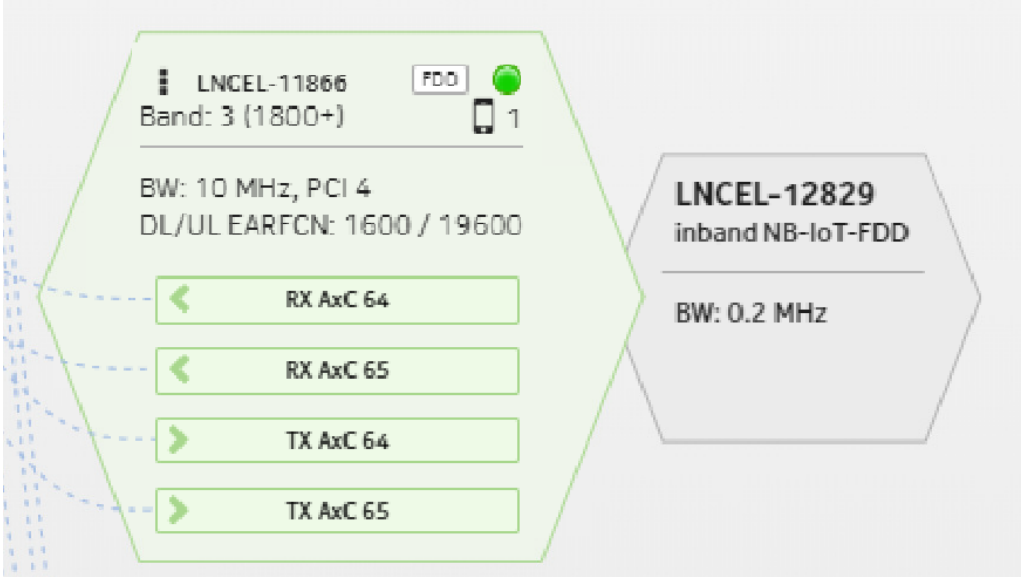
Figure 19 Site action options

Other icons that might appear on objects:

- 0 - active UEs in LTE cell
- - not configured hardware
- EXT - external ALD
- 5 - satellite count

In case any inband or guardband IoT cells are configured on the BTS, these are represented in Runtime View next to the hosting FDD-LTE cell.

Figure 20 IoT cells in Site Runtime View



3.1.3 Diagnostics view

> *The **Diagnostic** view is available only if the transport unit (TRS) is selected in **Site Runtime View**.*

Access to **Diagnostics** view: **Top Menu ► BTS Status ► Site Runtime View ► Detailed Site View ► select TRS object ► Diagnostics**

The following tests are available for the transport unit:

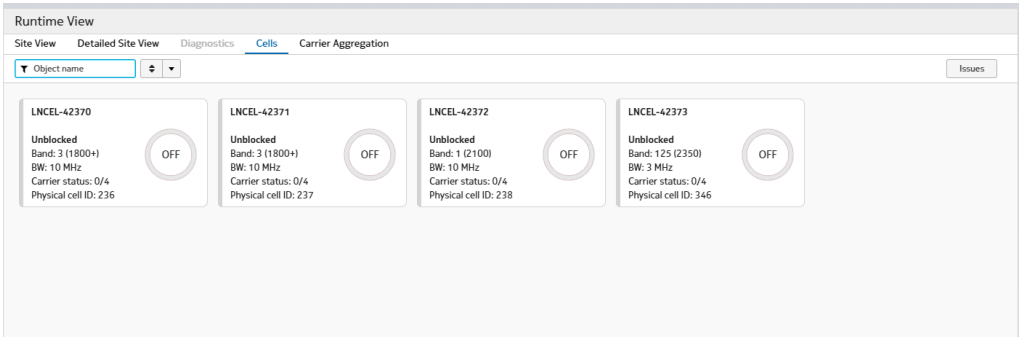
- Traceroute - tracks the route packets taken from an IP network on their way to a given host
- Short IPsec status - IP Security status
- Detailed IPsec status - detailed IP Security status
- IPsec configuration file - lists the IP security settings
- NTP server connection - Network Time Protocol (NTP) server connectivity test
- Neighbor entries - lists neighbor entries
- Routing info - lists entries in the kernel routing tables
- Interface settings - lists protocol addresses
- Address Resolution Protocol (ARP) table - displays the system ARP cache
- ETH link status - displays the status of all interfaces
- Networking sockets - lists the networking socket ports and respective services
- Numerical networking sockets - lists the numerical networking socket ports and respective services
- Routing table - displays routing table
- File system information - displays file system information

3.1.4 Cells view

*The **Cells** tab provides all the information about existing cells.*

Access to **Cells** view: **Top Menu ► BTS Status ► Runtime View ► Cells**

Figure 21 **Cells** tab



The **Cells** tab lists the cells currently configured on the site along with basic information about them. Full information about each cell appears in the **Details** panel after selecting a cell.

Percentages in a percentage gauge indicate the Trx or carrier status.

Cells statuses:

- Online - are displayed in a green color.
- Degraded - are displayed in an orange color.
- Offline - are displayed in a grey color.
- Failed - are displayed in a red color.

It is possible to sort cells by:

- Configuration ID
- Band
- State

To apply the issues filter, use the **Issues** button.

Cells can also be filtered manually, based on their name, ID, state, and so on, by using the text filter. Selecting any cell shows its details, such as basic information (state, name, and so on) and related parameters and faults when the **Details** panel is expanded.

If any alarm occurs in a cell, it will be indicated by the alarm icon (the color of the icon represents the severity of the alarm). In case of multiple alarms, the alarm icon on a particular unit indicates only the highest severity, although there may be other alarms. To see the list of alarms for that unit, go to the **Details** panel and open the **Faults** tab. To see even more details about the alarm, use the icon to go to the **Alarm Management** view. A list of alarms is also visible on a tooltip for that alarm.

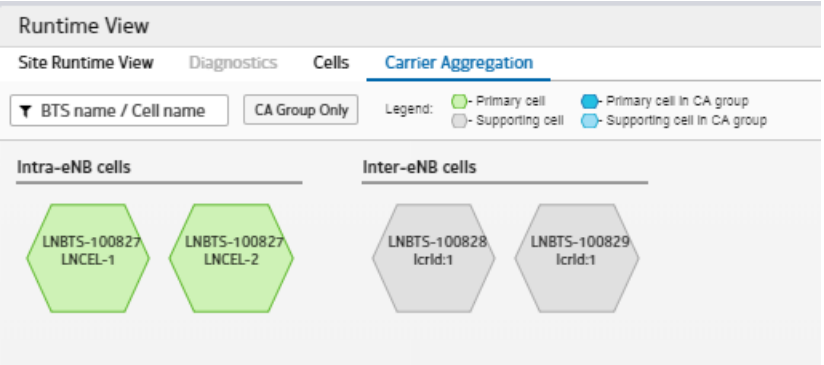
If a cell is locked, it is indicated by the lock icon. The icon marks a cell working in saving energy mode.

3.1.5 Carrier Aggregation view

*The **Carrier Aggregation** view displays cells connected to the BTS and cells from other BTSs configured as support cells.*

Access to **Carrier Aggregation** view: **Top Menu ► BTS Status ► Runtime View ► Carrier Aggregation**

Figure 22 **Carrier Aggregation** tab view



The **Carrier Aggregation** tab displays the BTS cells that WebEM is connected to as well as cells from other BTSs configured as support cells. Information about cells that are involved as supporting cells is taken from the configuration. Cells can be filtered by BTS name or cell name. The **CA Group Only** button applies a CA group only filter.

3.2 Data Streams by Cell or Carrier view

***Data Streams by Cell** and **Data Streams by Carrier** represent a physical and logical relation between physical and logical system units required to process signals.*

Access to **Data Streams by Carrier** view: **Top Menu ► BTS Status ► Data Streams ► Data Streams by Carrier**

Access to **Data Streams by Cell** view: **Top Menu ► BTS Status ► Data Streams ► Data Streams by Cell**

The **Data Streams** section represents a physical and logical relation between physical and logical system units required to process signals. As a result of the process, the BTS site can deliver the service to the user. The **Data Streams** view presents:

- Amount of functional data streams
- Status of processing signals
- Relations between HW units assigned to processing signals
- Basic identification information about detected HW units
- Availability status of HW units
- Operability status of functioning data streams

The information presented can be ordered by column name.

If an alarm occurs in a particular unit, it is indicated by the alarm icon (the color of the icon represents the severity of the alarm). In case of multiple alarms, the alarm icon on a particular unit indicates only the highest severity, although there may be other alarms. To see the list of alarms for that unit, go to the **Details** panel and open the **Faults** tab. To see even more details about the alarm, use the icon to go to the **Alarm Management** view. A list of alarms is also visible on a tooltip for that alarm.

Blocked objects are marked by the icon and locked objects are marked by the lock icon .

3.3 Site Report view

*The **Site Report** view shows a general report with site information.*

Access to **Site Report**: **BTS Status ► Site Report**

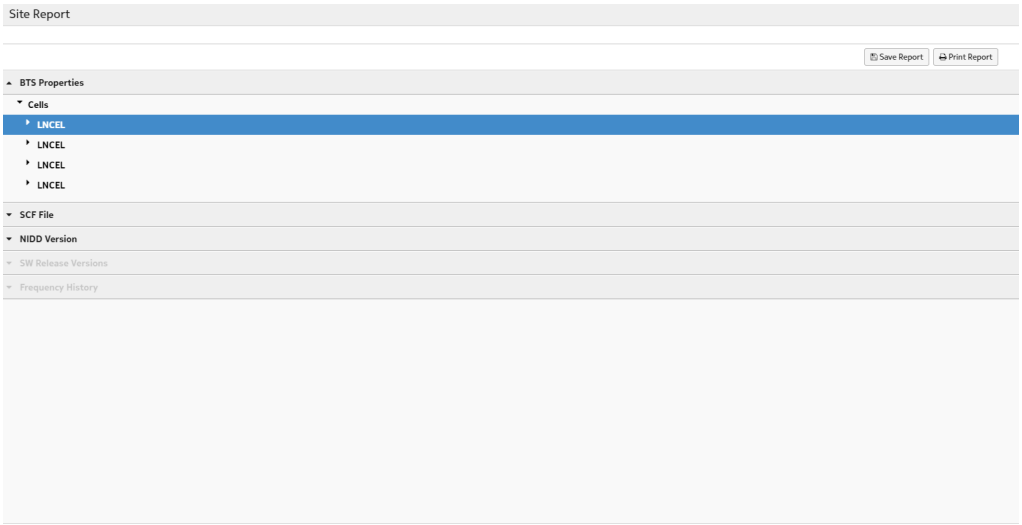
The **Site Report** view provides information about:

- BTS properties
  This section contains information about hardware and cells, for example: product code, serial number, status, antenna usage info, TRX or channel information and so on.
- SCF File
  This section allows to display an SCF in a separate browser window.
- NIDD Version
  This section provides information about the NIDD version in use.
- SW Release Version
  This section provides information about the software versions in use.
- Frequency History
  This section contains information about: time, source, average clock control value, tuning, difference, rejected samples and average number of GNSS satellites.

The **Save Report** button allows to save a report together with the SCF.

The **Print Report** button redirects an user to the printing dialog.

Figure 23 Site Report view



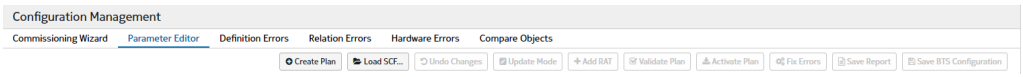
4 Configuration tab

Configuration provides a set of views to load, edit and save configurations as well as certificate management, reset configuration and RET management.

4.1 Configuration Management tab

*The **Configuration Management** section provides a set of functionalities to commission the BTS and resolve any errors that may occur during BTS configuration and commissioning.*

Figure 24 **Configuration Management** section



The **Configuration Management** section contains the following tabs:

- **Commissioning Wizard**
- **Parameter Editor**
- **Definition Errors**
- **Relation Errors**
- **Hardware Errors**
- **Compare Objects**

At the top of the view, the following buttons are available:

- **Create plan** - allows to create a new configuration.
- **Load SCF...** - allows to load a commissioning file or an SBTS16 snapshot file.
- **Undo Changes**
- **Update Mode** - the button is active in Frozen Mode and allows to exit it. Exiting the Frozen Mode causes the **Parameter Editor** to refresh and lose all implemented configuration changes.
- **Validate Plan** - performs the validation again and replaces the displayed validation errors (if any), using the *Planned value*, which is useful to verify the configuration before sending it to the BTS.
- **Activate Plan** - opens a pop-up window where clicking the **Execute** button sends the configuration to the BTS. To send the plan to the BTS, but not activate it, choose the **Download plan without activation** option before using the **Execute** button.
- **Fix errors** - the button appears only in the **Parameter Editor** tab and is active as long as there are any definition errors. It allows to fix errors by assigning default values to parameters, if they have any.
- **Save report** - the button is active after plan activation. Clicking the button starts downloading a ZIP file with XML and TXT files inside. These files contain information about the BTS state at the moment of the commissioning.
- **Save BTS configuration** - allows to save the currently edited configuration as an SCF.

4.1.1 Commissioning Wizard

*The **Commissioning Wizard** guides the user through the manual site planning and configuration.*

Access to **Commissioning Wizard** view: **Top Menu ► Configuration ► Configuration Management ► Commissioning Wizard**

Commissioning Wizard allows the user to have fully operational BTSs in the network by creating new configurations as well as editing existing ones, including inactive configurations, on the BTS or loaded from SCF. It is also possible to use Commissioning Wizard in offline mode (with or without a previously loaded IMS2 file).

Note: When all system modules, baseband modules and radio modules as well as the detected cables between them are commissioned, it is not possible to change the existing CABLINKs or manually create a new one. In this case, the cables in the configuration must fully correspond to the detected cables only.

Configuration can be performed via two channels: Commissioning Wizard site view and Commissioning Wizard modal view. Site view (topology view) provides the possibility to create basic modules and logical items (like cells) and establish connections between them. Modal view (configuration wizard) allows to create the same configurations as in the site view, but, additionally, more advanced parameters can be defined here.

Figure 25 **Commissioning Wizard** tab view

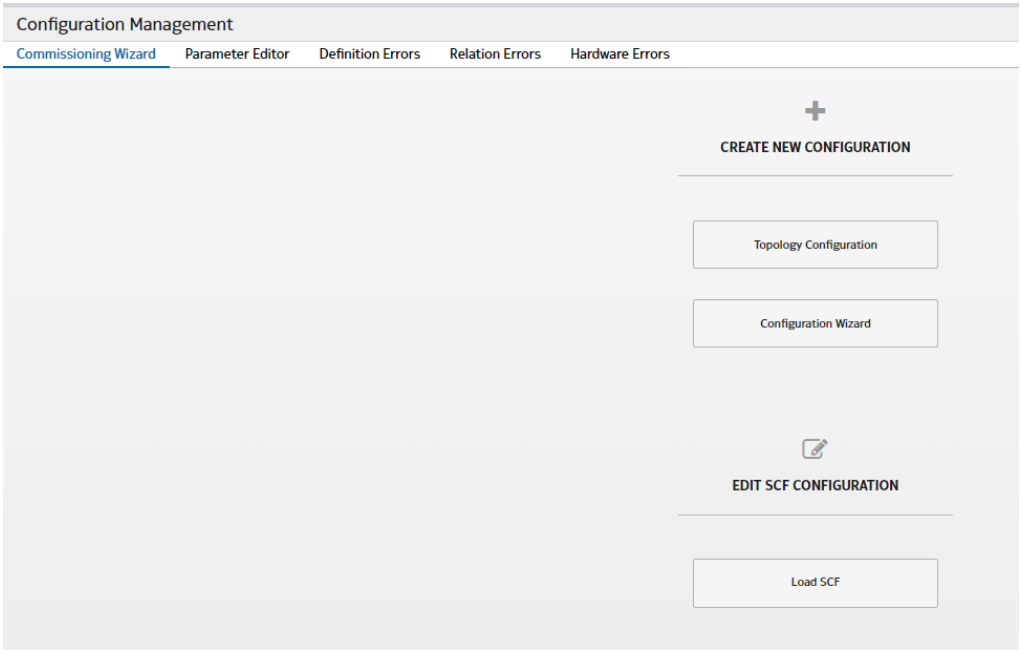


Figure 26 Example of commissioning step in **Commissioning Wizard** modal window view

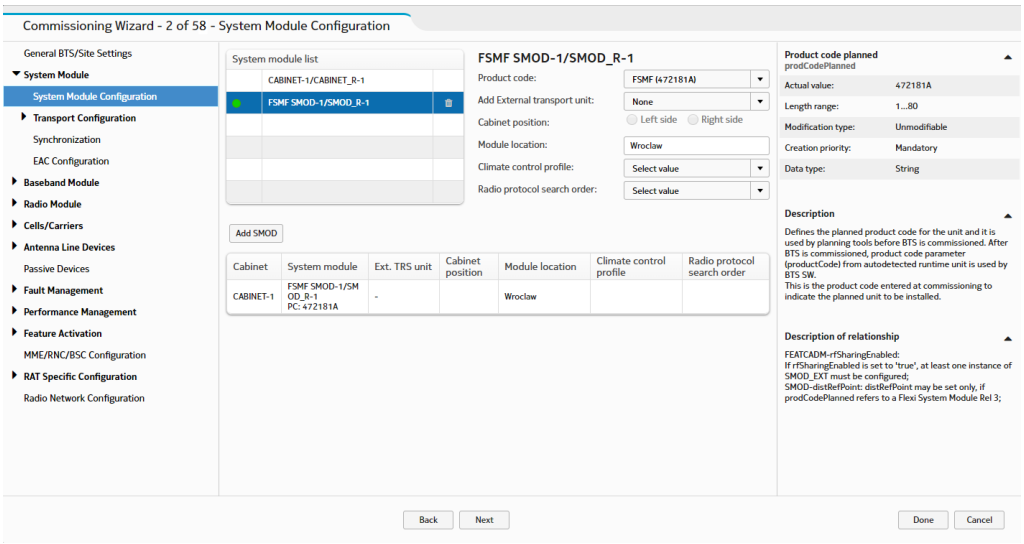
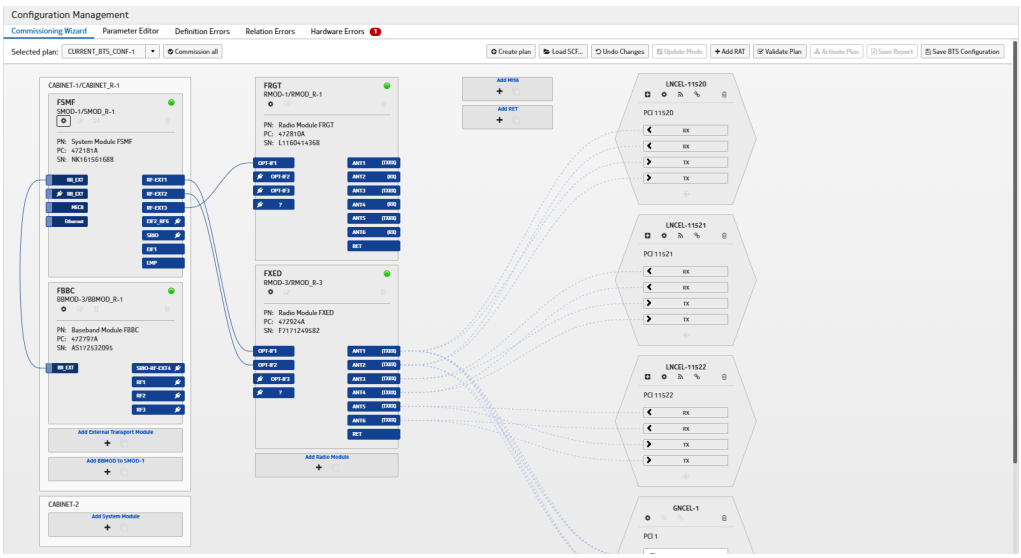


Figure 27 Example of site topology created with **Commissioning Wizard**



Commissioning Wizard uses a product code defined in a respective HW configuration object to identify a particular HW topology and capability. The product codes must be properly defined. If any HW unit product code is invalid, **Commissioning Wizard** reports it as an error and allows to fix it.

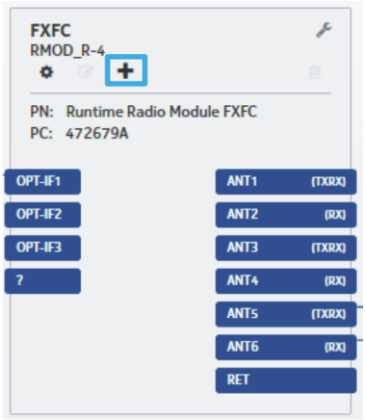
HW units are identified in **Commissioning Wizard** using HW type, configuration object identifier and runtime object identifier.

In **Commissioning Wizard** modal view, mandatory parameter errors and parameter relation errors are reported and visualized using error icons.

Commissioning Wizard works in offline and online mode.

Note: In online mode, WebEM detects existing hardware on a specific BTS site. Detected units are not automatically added to a configuration. To add an object to a configuration, use the + button visible on a particular unit or the same button, but in the Commissioning Wizard modal view respective page. If an object is already added, the button is not visible. To add all the objects, use the **Commission All** button.

Figure 28 Location of **Add Configuration** button



Commissioning Wizard site view

The **Commissioning Wizard** site view is divided into the working area panel, where the topology configuration can be performed, and the **Navigation Panel**, listing created objects (**Objects** tab). See Figure 27: Example of site topology created with Commissioning Wizard for reference.

To add a new hardware item or cell, use the respective + icon. To change any item in an existing configuration, use the respective icon. The icon opens the **Commissioning Wizard** modal view on the page corresponding with the item.

The icon is used to remove an item. This option is not available when a HW unit is detected and commissioned.

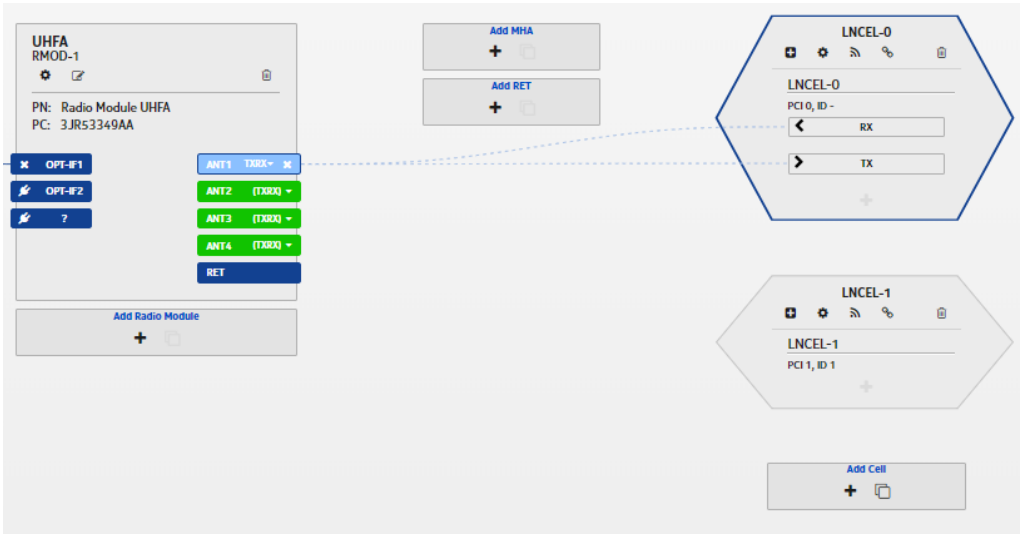
The icon visible in a cell object is used to add carriers. When used, the available antenna connections are highlighted in order to assign the carrier.

Physical and logical links can be created in the Commissioning Wizard site view. Clicking on any of the connectors starts the process of creating connections between units (LOGLINKs and CABLINKs). Green highlighted parts are available to establish connection, while the red highlighted button stops the connection process. Choosing the green button creates a connection. Click 

on the connector to remove the connection from the plan. A CABLINK can be removed from the configuration by clicking the respective **x** icon at baseband module side, but it is not possible to remove it from the radio module side when the cable is connected to the **?** port. Clicking the **x** at the baseband module side removes the respective CABLINK from the configuration (check in **Parameter Editor**), but the link remains visible in the runtime configuration in the Commissioning Wizard view. When planning logical connections between cells and radio modules, click on the add carriers icon (in a cell) and select the green highlighted connector to define the signal direction (TX/RX) on the radio module.

Figure 29 Example: connection between RF1 and OPT1 ports planned, selecting RF port for OPT2

Figure 30 Example: selecting signalling type for a cell carrier



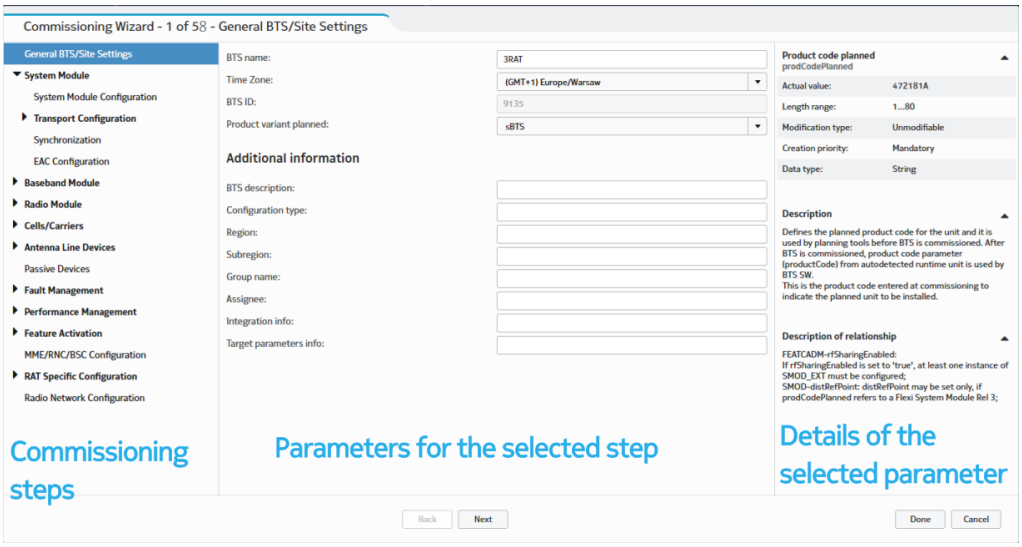
Connections, as well as physical and logical items, can be modified and removed at any time if the configuration is not activated. Note that, in case of a removal, all the related parameter settings already edited are lost.

Note: When all system modules, baseband modules and radio modules as well as the detected cables between them are commissioned, it is not possible to change the existing CABLINKs or manually create a new one. In this case, the cables in the configuration must fully correspond to the detected cables only.

Commissioning Wizard modal view

The **Commissioning Wizard** modal view is divided into three sections: commissioning steps, parameters for the selected step, and details of the selected parameter.

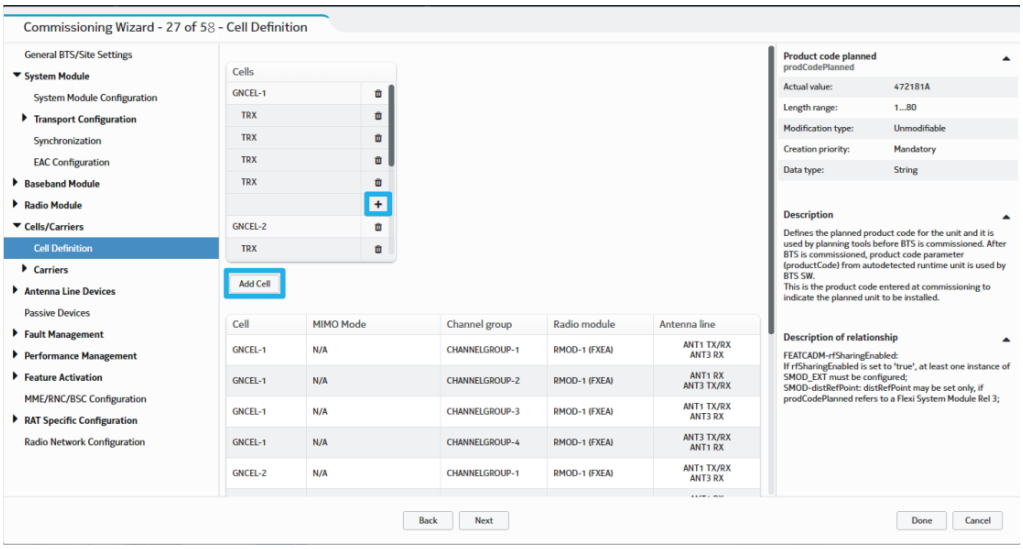
Figure 31 Sections in **Commissioning Wizard** modal view



To navigate through the wizard, use the **Back** and **Next** buttons. It is possible to freely navigate through the steps.

To add a new object to the configuration, use the respective button located under the table, for example: the **Add Cell** button. To add a new element to the object, use the + button located in the table. Those buttons are visible only where it is possible to add an object or element.

Figure 32 Adding a new object or element to the configuration

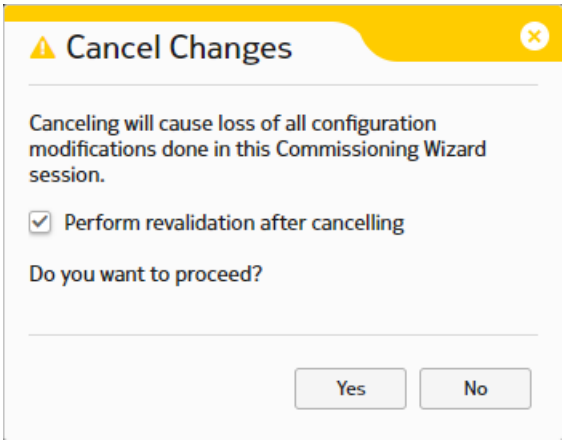


The **Done** button closes the window and saves the changes.

Note: The **Done** button does not send the configuration to the BTS. The configuration must be validated and then activated through the **Activate Plan** button in order to be applied on the site.

Cancel closes the window without saving. After canceling, the **Cancel Changes** pop-up window appears. Uncheck the option **Perform revalidation after cancelling** if needed and click **Yes** to proceed.

Figure 33 Cancel Changes

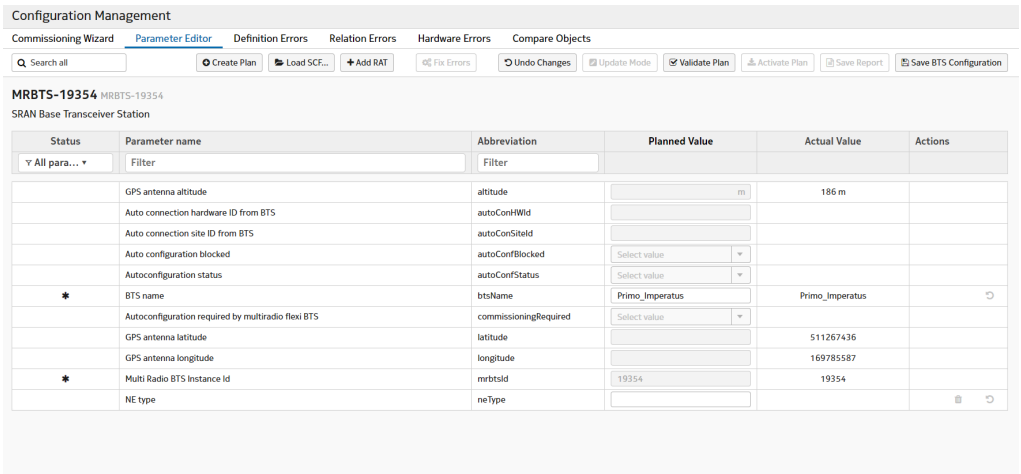


4.1.2 Parameter Editor

Parameter editor *allows to view and edit parameters from current or previously saved configurations from a Site Configuration File (SCF).*

Access to **Parameter Editor** view: **Top Menu ► Configuration ► Configuration Management ► Parameter editor**

Figure 34 **Parameter Editor** tab



Parameter Editor allows a generic parameter and object management (for example, setting only allowed parameter values) basing on a general BTS object model definitions.

Parameter Editor does not enforce a hardware specific limitations. For example, it allows setting not only parameter values supported by the given type of hardware. Hardware specific limitations are reported as errors in **Relation Errors** and **Hardware Errors** after desired parameter value is entered and plan is validated.

Parameters are used to configure and control the BTS site and are grouped into managed object (MO) classes:

- *Set by system* parameters user cannot change.
- *Mandatory* parameters are required for a BTS to work properly. When omitted, a message about missing or invalid parameter is displayed.
- *Optional* parameters are used to further configure the system.

WebEM provides functionalities necessary to easily find and edit necessary parameters as well as viewing parameter details.

Whenever parameter information is loaded from an SCF, validation is performed automatically in order to detect configuration errors such as not allowed or conflicting parameter values. Validation results are displayed in the **Definition errors**, **Relation errors** and **Hardware errors** tabs. Validation can also be performed manually by using the **Validate Plan** button.

To see parameters, an MO must be previously selected in the **Navigation Panel** ► **Objects**. After the MO selection, all assigned parameters are displayed along with the MO name. Note that not all MOs have associated parameters. In such cases, only the MO name is displayed, along with a `Parameters not available` notification.

Filtering parameters can be done in real time, using either of the following methods:

- The *Search all* text field - search by parameter name or abbreviated name through all the existing parameters.
- The following filtering options, available only for visible parameters:
  - Filter in parameter status column, by mandatory and optional parameters, and also by modified, invalid, existing and non-existing parameters.
  - Parameter name column text field.
  - Abbreviation column text field.

For example, selecting modified and invalid options parameters displays only parameters that have been modified with incorrect values.

To add a parameter, insert **Planned Value** for the chosen parameter. The new parameter is added after activating a configuration plan.

Parameters are displayed in a table view in alphabetical order. The first column shows parameter status:

- ✎ - Parameters that were modified; the new value is sent to the BTS after using the **Activate plan** option.
- 🗑 - Parameters marked for deletion; the parameters are deleted after using the **Activate plan** option.
- ⚠ - Parameter value is invalid.
- ✱ - Parameter is mandatory.

If the runtime configuration is loaded, the real values from the BTS are shown in the **Actual value** column.

The **Actions** column can be used to perform certain actions on the respective parameter:

- + - Add a structure
- − - Remove the structure
- 🗑 - Mark the parameter for deletion
- ↺ - Set the *Planned value* to the *Actual value*. If there is no *Real value* or the SCF is used, this action deletes the value
- ⚙ - Set the parameter to the default value

Using the ≡ (details) button expands the **Details** panel, displaying detailed information on the selected parameter, including validation errors (if any). The × (hide) button closes the pane.

Some BTS management operations, which can be performed by configuring certain NIDD objects and for which WebEM does not provide any dedicated views or functionalities, can be executed from WebEM by creating or configuring the desired NIDD objects and parameters in **Parameter Editor** and then validating and activating the planned configuration plan.

4.1.3 Conflicting commissioning data

Description of WebEM behavior when conflicting commissioning data occur

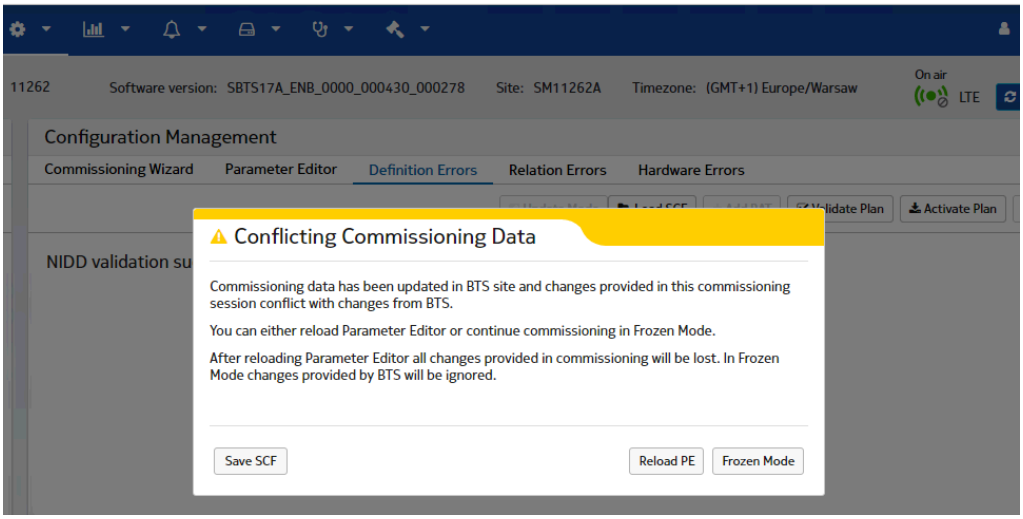
When changes in the **Commissioning Wizard** or in the **Parameter Editor** are performed, it is possible that commissioning data used by the BTS is modified in another WebEM session, in NetAct or internally by the system. Changes provided by the user in the **Commissioning Wizard** or in the **Parameter Editor** may conflict with changes applied to the system.

The WebEM behavior depends depends on the type of configuration conflict injection, as follows:

- When a delta or full recommissioning is performed via another WebEM session or via NetAct, it is impossible for WebEM to merge the changes implemented in the current session with the changes applied to the system, therefore it is only possible to save the backup SCF with the applied changes.
- When the changes are performed by the system (by configuring the SetByTheSystem parameters), WebEM merges the changes provided by the system with the changes performed by the user in a particular WebEM session. When the system modifies the same object class as the user, WebEM notifies the user about the conflict. When that happens, it is possible to either:
  - Switch to Frozen Mode
  - Refresh the changes (which causes the whole **Parameter Editor** to reload and all the changes provided by the user are lost)
  - Save the backup SCF with the changes applied to configuration used by the system before the conflict took place

In the Frozen Mode, the user can implement all the changes to the configuration before conflicting changes in the system are applied. After sending the changes to the system in Frozen Mode, a partial activation takes place and the plan is activated on BTS side. It is not possible to switch from the Frozen Mode to the Normal Mode without losing all the implemented configuration changes. It is not possible to enter Frozen Mode manually (this mode can only be entered when WebEM notices conflicting changes).

Figure 35 Conflicting commissioning data message



4.1.4 Validation errors (Definition, Relation, Hardware)

> *Validation error tabs are available after parameter validation is performed and if any errors have been detected.*

Access to **Validation errors** view: **Top Menu ► Configuration ► Commissioning wizard/ Parameter Editor ► Definition Errors/ Relation Errors/ Hardware Errors**

Validation is used to detect errors such as incorrect or missing parameter values, conflicting parameter values or parameter sets not matching configuration rules.

The same filtering and configuration options as in **Parameter editor** are available here.

Whenever parameter information is loaded (either from the current configuration or the SCF), validation is performed automatically in order to detect configuration errors such as not allowed or conflicting parameter values. Validation results are displayed in the **Definition errors**, **Relation errors** and **Hardware errors** tabs.

Validation consists of:

- XML validation - verifies file integrity and structure (in case of the SCF).
- NIDD validation - detects incorrect parameter values or missing mandatory parameters.
- Parameter relation error validation - detects conflicting parameter values.
- Hardware validation - detects incorrect hardware-related parameter values, conflicting with the planned or actual hardware used on the site.

Validation errors, if any, are grouped into three categories and displayed separately:

- **Definition errors** lists errors such as unknown parameter or MO names, missing mandatory parameters or mandatory values, incorrect values. When definition errors occur, plan activation is not possible. Parameter values can be modified directly from this view.
- **Relation errors** lists errors related to relationships between parameters or parameter sets. For example, when a certain parameter value conflicts with another.
- **Hardware errors** lists errors related to the planned or actual hardware configuration. For example, when hardware-related parameter values do not match the hardware used on the site (such as serial number, unit name and so on).

Note: WebEM gives the user tips on how to repair errors according to PDL validation rules.

It is possible, but not recommended, to activate a plan with relation or hardware errors. Nokia does not take responsibility for plan activation failure in case the plan is activated with relation or hardware errors.

4.1.5 Compare Objects

*The **Compare Objects** functionality allows comparison of different configurations.*

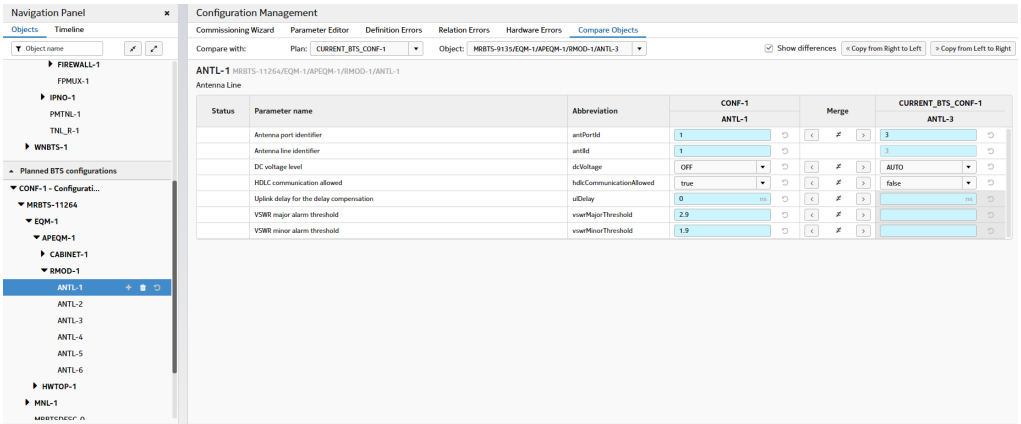
Access to **Compare Objects** view: **Top Menu ► Configuration ► Configuration Management ► Compare Objects**

The **Compare Objects** functionality allows comparison of different configurations. To compare parameters, more than one configuration is required. Select the managed object class (MOC) in the **Objects** tab in the **Navigation Panel** and then choose **Plan** and **Object** from the respective drop-down lists in the **Compare with** menu.

If the **Show differences** check-box is marked, only parameters with different values are visible.

The **Copy from Right to Left** and **Copy from Left to Right** buttons allow copying values of all compared parameters from one configuration plan to the other. To copy a single parameter, use the **<** or **>** button in the **Merge** column. To revert a parameter to its previous value, click the  icon.

Figure 36 Compare Objects window



4.2 Certificate Management tab

*The **Certificate Management** view allows to manage certificates and their functions.*

Access to **Certificate Management** view: **Top Menu ► Configuration ► Certificate Management**

The **Certificate Management** functionality offers a common way to manage certificates and their functions. Certificates are used to ensure that a public key comes from a trusted authority. A certificate contains information about the owner of the certificate, owner's name, certificate usage, duration of validity, resource location or Distinguished Name (DN) which includes the Common Name (CN) and the certificate ID of the person who certifies (signs) this information. It contains also the public key, and finally a hash to ensure that the certificate has not been tampered with. To see detailed info about each certificate click on the relative row in certificate table. All information is displayed in the **Details** panel.

The Certificate Authority maintains a list of all signed certificates as well as a list of revoked certificates (CRL). A certificate is insecure until it is signed, as only a signed certificate cannot be modified. A CMP server must be configured to manage certificates automatically.

When a BTS certificate is changed, the browser may fail to validate the SSL certificate. In that case, WebEM cannot set up a new HTTPs connection, which may result in, for example, file transmission failure. Refresh the web page and manually accept the certificate to solve this issue.

4.2.1 BTS Certificates view

*The **BTS Certificates** view allows to manage BTS certificates.*

Access to **BTS Certificates** view: **Top Menu ► Configuration ► Certificate Management ► BTS Certificates**

The **BTS Certificates** tab shows information about certificates on the BTS in a table format:

- Status - certificate status
- Issued to - to whom the certificate is issued
- Issued by - who has issued the certificate
- Type - certificate type
- Valid from - the starting date of the certificate's validity
- Valid to - the ending date of the certificate's validity
- Serial number - certificate's serial number

You can use to collapse all the information in the table or  to expand all. The **Delete** button is used to delete the selected certificate from the table (the BTS trust chain cannot be deleted).

To install a new certificate, select the BTS trust chain and additional CA certificates by using the **Browse** button. Passwords must be provided if required (depending on the type). Use the **Install** button to use the selected certificates.

4.2.2 Automatic Management view

*The **Automatic Management** view allows to configure automatic certificate management.*

Access to **Automatic Management** view: **Top Menu ► Configuration ► Certificate Management ► Automatic Management**

The **Automatic Management** tab displays the Certificate Management Protocol (CMP) Server information. This tab is available only if the CMP server is supported.

CMP/CA server settings:

- Reference number - CMP server reference number value. Clicking the **Import** button opens the file selector.
- Pre-shared key - CMP server pre-shared key value. Clicking the **Import** button opens the file selector.

Click the **CMP Key Update** button to trigger the CMP key update request. This button is disabled when the CMP server address or port is not configured or there are unsaved changes in the UI. CMP Key Update is disabled also when the BTS certificate has expired or there is no BTS certificate installed.

Click the **Initialize Certificates** button to trigger the CMP initialization request. This button is disabled when the CMP server address or port is not configured, when there are unsaved changes in the UI, or when there is no CA certificate in the BTS certificate chain and a CA subject name has not been configured.

4.2.3 Certificate Revocation Lists

*The **Certificate Revocation Lists** view shows the list of revoked certificates.*

Access to **Certificate Management** view: **Top Menu ► Configuration ► Certificate Management ► Certificate Revocation Lists**

Clicking the **Update Revocation List** button triggers the CRL initialization request.

- CRL issuer - name of the CRL issuer
- Updated - when the CRL has been updated
- Next update - when the CRL will be updated next
- Revoked certificates - the number of revoked certificates
- Distribution point - CRL distribution point URL
- Type - CRL distribution point type
- Failure reason - failure reason if the download has failed

4.2.4 Vendor Certificates view

*The **Vendor Certificates** view contains the list of the vendor certificates.*

Access to **Certificate Management** view: **Top Menu ► Configuration ► Certificate Management ► Vendor Certificates**

- Status - certificate status
- Issued to - to whom the certificate is issued
- Issued by - who has issued the certificate
- Type - certificate type
- Valid from - the starting date of the certificate's validity
- Valid to - the ending date of the certificate's validity
- Serial number - certificate's serial number

You can use to collapse all the information in the table or to expand it all. Clicking the **Restore Vendor Certificates** button restores vendor certificates in use in the BTS. The button is disabled if there are no vendor certificates. For more details about a particular certificate, expand the **Details** panel.

4.3 CBRS Certificate Management tab

CBRS Certificate Management description

Citizens Broadband Radio Service (CBRS) Certificate Management provides the possibility to install certificates necessary to activate CBRS feature. This functionality contains two tabs:

- CBRS Certificates
- CBRS Certificate Revocation Lists

Note: These tabs are available for configurations with an AirScale system module. FSMF is not supported.

4.3.1 CBRS Certificates view

*The **CBRS Certificates** view allows to generate certificate signing request (CSR), install and display CBRS certificates.*

Access to **CBRS Certificates** view: **Configuration ► CBRS Certificate Management ► CBRS Certificates**

This view provides the possibility to install CBRS certificates and display the ones that are already installed. To perform this operation click the **Browse** button next to **CBRS vendor chain**, select the proper file and click **Open**. Repeat the steps for **Additional CA certificates** if required. Click **Install**.

Installed certificates are presented in a table containing the following information:

- Status
- Issued to
- Issued by
- Type

- Valid from GMT +01:00
- Valid to GMT +01:00
- Serial number

This view also allows to generate a certificate signing request (CSR), by clicking **Generate CSR**, copy or save CSR.

4.3.2 CBRS Certificate Revocation Lists

*The **CBRS Certificate Revocation Lists** view shows the list of revoked certificates.*

Access to **CBRS Certificates** view: **Configuration ► CBRS Certificate Management ► CBRS Certificate Revocation List**

The **BTS Certificates** tab shows the following information for revoked CBRS certificates in a table format:

- Issuer
- Updated GMT +01:00
- Next updated GMT +01:00
- Revoked certificates
- Distribution point

4.4 Configuration Reset view

Configuration reset clears the system module from any parameter settings, which can be used, for example, when a module must be moved to another site. Configuration reset is unavailable in remote connection.

Access to **Configuration Reset** view: **Top Menu ► Configuration ► Configuration Reset**

The **Execute Reset** button located in this tab allows to reset configuration. Reset can be performed with removal of security credentials.

The configuration reset clears the configuration on both partitions (active and passive). This means that the BTS is not commissioned after the rollback or fallback procedure if the configuration reset was performed.

Note: Configuration reset is unavailable in remote connection.

4.5 Centralized RET Management view

*The **Centralized RET Management** tab is used to manage the RET unit configuration, without the need to go into **Commissioning Wizard** and activate a plan.*

Access to **Centralized RET Management**: **Top menu ► Configuration ► Centralized RET Management**

The **Centralized RET Management** tab allows to change RET unit configuration directly, without the need to go into **Commissioning Wizard** and activate a plan. The main functionality of this view is changing planned values of angles and calibration. There are three visible angles values: planned value, current plan value and actual value. Additionally, RET configuration changes can also be done by uploading a configuration file (BIN file) to the device. These files contain configurations of all angles as well as additional information about the RET. Settings can be sent to a BTS by using the **Send** button. The action state is visible in one of the columns in this tab. When an action is completed, new angles are displayed along with possible errors. For more details, parameters, faults or options about the selected Antenna Line Device or RET, open the **Details** panel.

4.6 IPSec PSK Configuration view

*The **IPSec PSK Configuration** tab allows to input a pre-shared key.*

The **IPSec PSK Configuration** tab allows to input a pre-shared key. This key can be typed into a field or imported using the **Import...** button. The imported file must be in XML or TXT format.

The pre-shared key must fulfill the following requirements:

- A minimum of eight and a maximum of 128 characters.
- At least two numbers, both upper and lower case characters, no two identical characters consecutively.
- At least one non-alphanumeric character except space and quotation mark """.

The **Update** button is active only after setting up a pre-shared key.

4.7 Centralized RAE Management view

*Description of the **Centralized RAE Management** tab.*

Access to **Centralized RAE Management**: **Configuration ► Centralized RAE Management**

Centralized RAE Management tab allows the user to manage the Remote Antenna Extension (RAE) device selected from the list. The user can set the values of:

- Frequency
- Beamwidths (vertical and horizontal)
- Angles (downtilt and azimuth)
- Weight factors

These values can be set automatically by using the **Get Beamwidths**, **Get Angles** and **Get Weight Factors** buttons.

Note: The **Get Beamwidths** button is enabled when the **Frequency** is set. To enable **Get Angles**, **Frequency** and **Beamwidths** must be chosen. The button **Get Weight Factors** becomes active when all the other parameters are set.

The **Update Weight Factor File...** button opens a file browser to select the Weight Factor File.

The **Restore Factory Defaults...** button restores the weight factors for the selected unit.

In the **Centralized RAE Management** tab there is a list of the files with RAE parameters. The user can save these files by clicking the **Save** button.

5 Performance tab

> ***Performance*** *provides a set of views to monitor BTS-related counters and measurements.*

5.1 Performance Management view

Access to **Performance Management** view: **Performance ► Performance Management ► BTS Counters / Transport Counters / Real-time Measurements**

Performance Management contains the following tabs: **BTS Counters** (opened by default), **Transport Counters** and **Real-time Measurements**. Performance data is gathered and presented in real time for as long as WebEM is connected to the BTS.

After selecting an object from the **Navigation Panel ► Objects**, the related counters and their values are displayed in either table view or plot view. The **Table/Plot View** button is used to switch between the two. The selected counters are listed in the **Details** pane, each counter with a different color assigned. The detailed value is displayed once clicked on the chart. Up to 20 items can be displayed at the same time. The data are displayed for the time intervals specified in a **Display data for** drop-down list.

Figure 37 Table View

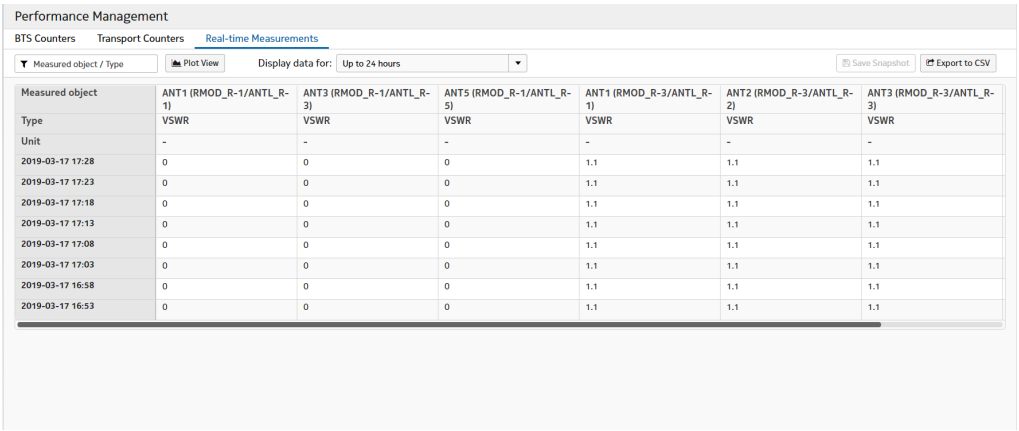
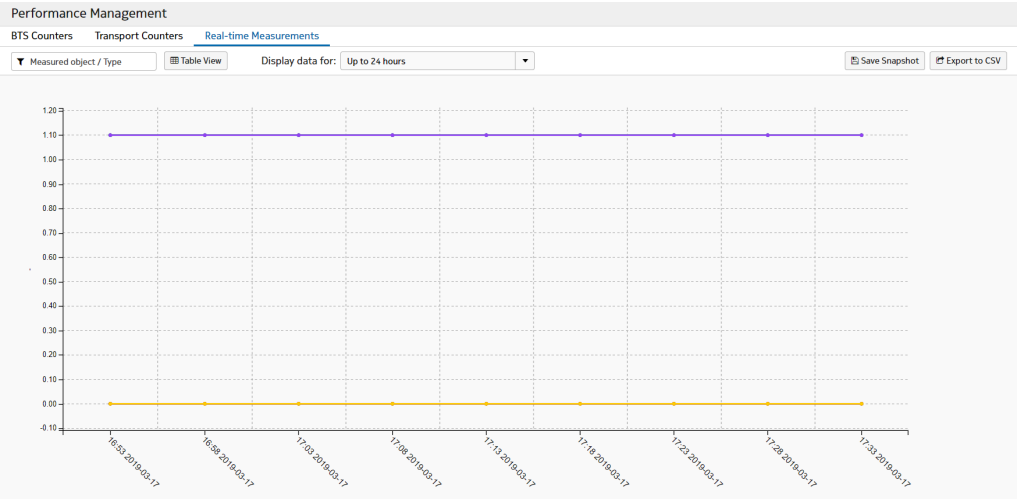


Figure 38 Plot View



The date and time from performance measurement (BTS) are used for BTS counters and TRS counters. Real-time measurements are displayed in the BTS time.

In online mode (when WebEM gathers data from the BTS), the **BTS Counters** tab shows historical values in table view and real-time data in chart view by default. It is possible to show values for a selected timespan, when one is selected from the **Navigation Panel ► Timeline**. For BTS and TRS counters, all data gathered up to the current timestamp is available.

In offline mode, when data is loaded from a snapshot, the **BTS Counters** tab shows the latest value and saved data in a chart view by default. It is possible to show values of real-time and hardware monitoring for a selected timespan, when one is selected from the **Navigation Panel ► Timeline** panel. For BTS and TRS counters, all the data gathered up to the current timestamp is available.

When IMS2 is used, only real-time measurements and hardware monitoring are available. When a snapshot is used, PM files are also available, and data from all PM files from the snapshot is displayed.

Items in **Navigation Panel** can be filtered by name. Users can also manually select counters and save a filter as an XML, by using the **Export filter** button in **Navigation Panel**. To load a saved filter, click **Import filter**.

The **Save Snapshot** option allows to save the currently visible graph as a PNG file (only in graph view).

Export of BTS counters can be done by using the **Export to CSV** button.

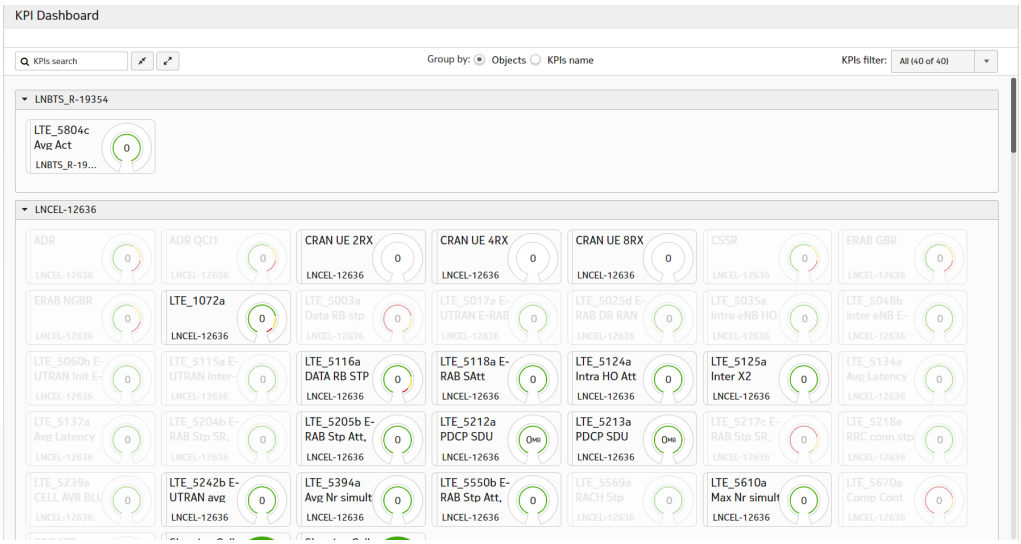
5.2 KPI Dashboard

> ***KPI Dashboard*** *view allows to see respective KPIs for all objects.*

Access to **KPI Dashboard** view: **Performance ► KPI Dashboard**

KPIs are displayed for objects selected in **Navigation Panel ► Objects**. The dashboard can be grouped by objects or KPI name. KPIs can be filtered, by using the KPI filter, ordered either by name or by related object, and searched by name. The list of all KPIs can be collapsed and expanded. The **Details** panel displays details for all the selected KPIs.

Figure 39 **KPI Dashboard**



6 Alarms in WebEM

__Alarm Management__ allows to see details on active BTS faults as well as fault history

Access to **Active Alarms** view: **Alarms ► Alarm Management ► Active Alarms**

Access to **Alarm History** view: **Alarms ► Alarm Management ► Alarm History**

Alarm Management is divided into two tabs: **Active Alarms** showing the actual (real-time) data about BTS faults, and **Alarm History** showing the historical data. Both tabs are configured and navigated in exactly the same way.

Note: The alarms in the **Alarm History** tab are available only when history is loaded in the **Navigation Panel**. For more information, see The Navigation Panel topic.

Details of a selected alarm, such as time of appearance, description, and instructions on how to deal with the fault, are visible in the **Details** panel.

Alarms can be sorted using the text field and ordered by severity or impacted RAT using the **Appeared** column.

The **Show Source** button in the **Details** panel navigates to the **Detailed Site View** and selects the alarming object.

The **Objects** tab in the **Navigation Panel** can be used to filter alarms by the related managed object.

Historical information goes back to a maximum of 24 hours or the last BTS reset.

Faults can be filtered by using:

- Text field to filter any alarm names, IDs, dates, alarming objects containing the provided text fragment.
- Alarm type:
  - Critical alarms, presented by the icon
  - Major alarms, presented by the icon
  - Minor alarms, presented by the icon
  - Warnings, presented by the icon

Additionally, the information presented in the table can be ordered by selecting column and saving to a CSV file by using the **Save** button: .

Note: Alarms before NTP synchronization can have incorrect timestamps, which are not updated after NTP synchronisation.

Fault Toggling History

Fault toggling is a functionality that allows the user to suppress alarms that are raised and cleared in a short period of time, thus having no further impact on the fault analysis. This view enables generating and saving a Fault Toggling History report.

7 Software Management tab

*The **Software Management** view allows to view and update software currently used on the BTS site.*

7.1 Software Version view

This tab allows to view the software version of the BTS and technologies configured on the site.

Access to **Software Version** view: **Software ► Software Management ► Software Version**

This tab allows to view the software version of the BTS and technologies configured on the site.

7.2 Software Update view

*The **Software Update** view allows to update software version.*

Access to **Software Update** view: **Software ► Software Management ► Software Update**

This tab allows to update and use the BTS site software, RFM plugin software and ALD software. The contents of the SW package are defined in a master file (SW package ZIP file). A SW update may need to be performed to add some new features to better support customer needs, to replace SW with bugs, or to guarantee compatibility with other element types due to their own SW upgrade. You can view the current SW versions in the **Software Version** tab.

⚠ Do not disconnect any unit, power supply or WebEM during the software update procedure. Any interference during the software update procedure may damage the hardware severely.

Note: If the SW update is ongoing, changing the WebEM view does not stop the operation. When switching back to the **Software Management** view, the software update is still ongoing if is not finished.

Note: Clicking the **Cancel** button aborts the software download.

The passive, active and planned software versions are displayed at the top of the view.

Click the **Rollback...** button to change between active and passive software versions (to revert to the previously used SW version). The button is disabled if an update or a rollback is ongoing or passive software version information is not available.

Click **Backup BTS Site Configuration** to save the site configuration file (SCF) to a local drive.

The BTS site software can be updated either from a local drive or a remote server by selecting the appropriate software source option. In case of a local drive, the local file must be selected using the **Browse** button. In case of a remote server, a URL address to the file location must be provided. Once the software ZIP file is selected, it is loaded to WebEM, where the user can see the software details.

Save SW History Report is used to save the recorded SW history to TXT file.

Clicking the **Start** button uploads the selected and loaded software package to the BTS. Selecting the **Activate software after update** checkbox takes the selected version into use, otherwise the new SW version is listed as planned. This action results in a BTS restart. After the restart, a new software version is used and marked as active, and the previously used version is marked as passive. The progress and elapsed time of the software update progress is displayed. The **Cancel** button allows to cancel a SW download

The SW update time depends on the file size. The update progress shows the transfer status of files. A notification is displayed after completion.

If **Activate software after** update is left unchecked, the new software is still downloaded to the BTS Site but the site does not restart. To activate the software later, go through the update procedure again with Activate SW after update checked. This time WebEM does not download the files that already exist on the BTS site.

Save SW Update Report is used to save the latest update report to TXT file.

Note: During the SW update, the connection to the BTS is lost and, if the certificate is not validated, the user must refresh the browser after the SW update procedure, otherwise the connection to the BTS is not reestablished automatically. After the SW upgrade, the BTS certificate may change and it is recommended to refresh the browser to obtain the new certificate.

7.3 Antenna Line Devices Software view

*The **Antenna Line Devices Software** view allows to create antenna line device (ALD) software based on detected ALDs or by updating existing ALD software.*

Access to **Antenna Line Devices Software** view: **Software ► Software Management ► Antenna Line Devices Software**

This tab allows to create ALD software based on detected ALDs or by updating existing ALD software. It is possible to restore HW info with or without a serial number, by using a drop-down list. The **Import Existing File...** button allows to upload a ZIP or XML file.

- SW file - in this column you can select a software file using icon
- Manufacturer
- Product code - this column also allows for ascending or descending ordering
- Serial number
- HW version
- Target SW version

- SW update options - the user can choose one option from a drop-down list: Normal, Restricted or Forced

Additional autodetected information on hardware, such as name, type and current software version, is displayed in the **Details** panel. This information stops being displayed synchronously with the BTS once the user edits the ALD SW table.

8 Diagnostic tab

*The **Diagnostic** view allows to set and execute tests, a swell as use a terminal and create reports.*

8.1 Synchronization view

*The **Synchronization** view has three tabs: **Status**, showing the actual (real-time) details on synchronization, **Tuning**, allowing to configure synchronization tuning, **Test Clocks**, allowing to synchronize the external RF measuring equipment.*

Access to **Synchronization** view: **Diagnostic ► Synchronization**.

Status

Status displays the actual (real-time) details on the synchronization source and time servers. It also shows the synchronization source detailed status, such as synchronization hub, synchronous Ethernet, and Timing over Packet (ToP) status as well as GNSS satellite information.

The **Details** panel displays the **Synchronization hub** and **Timing over Packet** details.

Tuning

Fast tuning can be used if the BTS clock must be adjusted or the user wants to synchronize the BTS clock quickly. To start the fast tuning, select the **Fast** option and click the **Tune** button.

Note that if the system module operates as a synchronization slave, it is not possible to tune the BTS clock.

Tuning the BTS clock manually is used for the following purposes:

- To read the current digital-to-analog converter (DAC) word from the BTS or to change the current DAC word on the BTS.
- To browse the history information about the difference between BTS clock and external reference clock frequency to find out the frequency stability or accuracy.

If the BTS determines that the reference signal quality during fast tuning is insufficient, fast tuning is interrupted and the BTS continues with normal tuning.

The **Get History** button allows the user to view the history information about the difference between the BTS clock and the external reference clock frequency to find out the frequency stability or accuracy. It is also possible to save and print the history information, using the respective buttons.

Note that there can be entries with the date 01.01.2004 in the frequency history file. This date is shown if Network Time Protocol (NTP) time has not been available.

Test Clocks

Test Clocks allow to test the functionality of the test clock output signal in the SYNC OUT connector of the BTS. It is also possible to enable or disable the frame clock output signal and to select which frame clock is used (100 Hz, 50 Hz, 25 Hz, 12.5 Hz or SFN0). The clock signal is used for synchronizing external RF measuring equipment and must be disabled during a normal BTS operation.

The current status of the 10 MHz test clock is visible at the top of the view. Use the **Enable** checkbox to enable or disable the test and select which frame clock is used with the **Output** list. The **Send** button saves the settings.

8.2 IP Connectivity Test

> ***IP Connectivity Test*** *allows to test ping connections to certain configured remote host addresses.*

Access to **IP Connectivity Test** view: **Diagnostic ► IP Connectivity Test**

To do an IP connectivity test, fill in the following settings:

- Scope - choose one option from a drop-down list. The possible options are:
  - **User-defined address (default)**
  - **All configured hosts**
  - **All configured IPv4 hosts**
  - **All configured IPv6 hosts**
  - **BFD <Y> x.x.x.x**
  - **CMP/CA server x.x.x.x**
  - **<IPRT-Y | IPRTV6-Y> routing default gateway x.x.x.x**
  - **NTP server x.x.x.x**
  - **Primary BSC x.x.x.x**
  - **Primary DNS server x.x.x.x**
  - **Primary LDAP x.x.x.x**
  - **Primary MME x.x.x.x**
  - **Primary OAM x.x.x.x**
  - **Real-time PM collection entity x.x.x.x**
  - **Remote syslog server x.x.x.x**
  - **RNC**
  - **RTT Measurement session <Y> x.x.x.x**
  - **Secondary BSC x.x.x.x**
  - **Secondary DNS server x.x.x.x**
  - **Secondary MME x.x.x.x**
  - **SGW x.x.x.x**
  - **ToPF ToP master x.x.x.x**
  - **ToPP ToP master x.x.x.x**
  - **RNC x.x.x.x**
- **Address** - only used and mandatory in case of a user-defined address scope.
- **Source address** - choose an address from a drop-down list.

- **Payload Size** - bytes [16...61411]
- **DSCP** - [0...63]

Press **Start** to display the test result in the table below. To stop testing, press **Stop**.

Note that a test failure does not always mean there is no connection. Various scenarios must be taken into consideration. Therefore, make sure to select the correct source address.

8.3 RF Diagnostic Test

> ***RF Diagnostic Test*** *allows to test and verify the RF characteristics of RF modules.* ***RF Diagnostic Test*** *is supported for rel. 2 or newer HW.*

Access to **RF Diagnostic Test** view: **Diagnostic ► RF Diagnostic Test**

The **RF Diagnostic Test** view contains two tabs: **Test Setup** and **Test Result**. RF diagnostic is valid on LTE RAT only.

Test Setup

To execute the test, select which cells are to be tested (all or an individual cell) and define thresholds for the BTS:

- RF Power Error High Threshold (dB)
- RF Power Error Low Threshold (dB)
- RTWP High Threshold (dBm)
- RTWP Low Threshold (dBm)
- TX Antenna VSWR High Threshold

Activate remote RF diagnostic test is marked by default.

To define thresholds for bands, click the + icon and fill the required parameters (Band class, Total RF power high threshold, Total RF power low threshold). To delete thresholds for bands, use the 🗑 icon.

The **Save threshold** button sends the configured threshold to the BTS.

Use **Start Test** to initiate the test. The progress and results are displayed in the **Test Result** tab when available.

Test Result

The **Test Result** tab contains a table with general test information and a table with a detailed result for each antenna. Test results are displayed for selected cells. The list of cells is in the left table and can be filtered by local cell ID. Test results can be saved for one cell (**Save Cell Results**) or for all sells (**Save All Results**). Results are saved in a text file.

8.4 EAC Functionality Test

EAC Functionality Test *allows to test the functionality of the External Faults and Controls (EAC) for the commissioned BTS. If the SW update is in progress, the test cannot be run. The information for the test is checked from the site configuration file.*

Access to **Functionality Test** view: **Diagnostic ► EAC Functionality Test**

This view contains two tabs: **Faults** and **Controls**.

Note that only commissioned EAC lines can be tested in EAC Functionality Test.

Faults are used to test external fault lines, if EAC is configured. Select the lines to be tested in the **Selected to test** column and the results are updated when available. Using the **Save Results** button allows to save the results to the TXT file.

Controls are used to test the external control lines. Change the state of the output line and click **Send** to send the changes to the BTS. After the BTS has changed the state of the external control line, check the state of the supervised external device. The operator can update test results in the **Test result** column. Using the **Save Results** button allows to save the results to a TXT file.

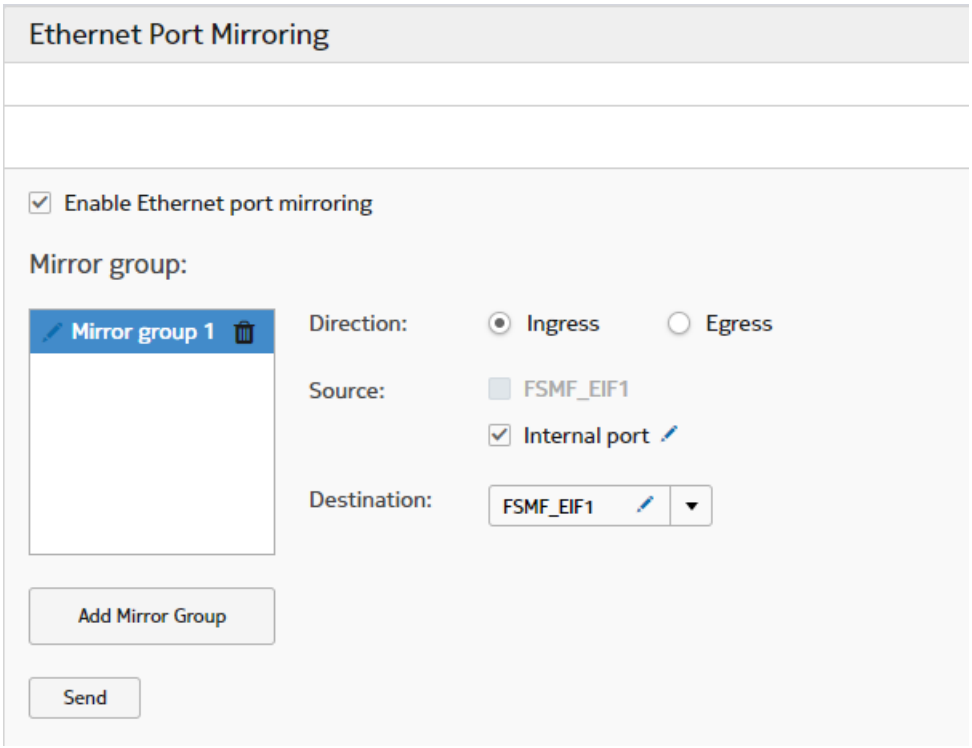
8.5 Ethernet Port Mirroring

Ethernet port mirroring *is used for identifying, monitoring and troubleshooting network abnormalities. The traffic that emerges to and from specific port number is automatically copied and transmitted to a monitoring port.*

Access to **Ethernet Port Mirroring**: **Diagnostic ► Ethernet Port Mirroring**

To enable Ethernet port mirroring, mark the checkbox **Enable Ethernet port mirroring**. Click **Add Mirror group** and set direction, source and destination for the mirroring. Clicking the **Send** button applies the changes to the configuration plan and triggers its validation and activation. No BTS reset is required.

Figure 40 Ethernet Port Mirroring



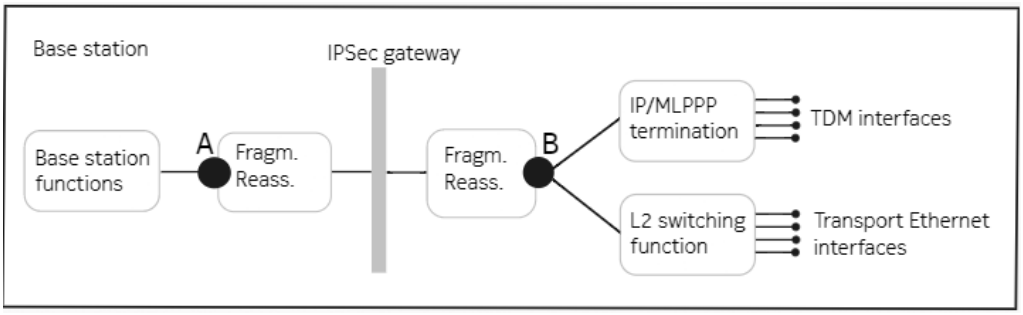
8.6 IP Traffic Capturing

IP Traffic Capturing allows to capture the traffic to and from a local port into a file or stream towards another port

Access to **IP Traffic Capturing** view: **Diagnostic ► IP Traffic Capturing**

To capture traffic at transport network interface level, select one of the capture point options. For more information, see Figure 41: Capture point options for IP traffic capturing

Figure 41 Capture point options for IP traffic capturing



Selection of a capturing point depends on the intended packets to be monitored. When IPSec is configured, if we capture trace at point A, we are able to capture packets before IPSec encryption. If we capture trace at point B, then we are able to capture the packets after IPSec encryption.

The following options are also available:

- **Include U-plane** - includes user plane traffic
- **Output** - allows to define the data output: save the data to a file (and optionally protect it with a password) or stream the data to another port.

Clicking on **Start** initiates the capture. The status and duration are displayed. The **Stop** button stops the process. The BTS automatically stops the traffic capturing after 24 hours if the user does not stop it. The captured data is saved on the BTS, and is generated as a file only if the user clicks the **Generate and Download File** button.

8.7 SFP Monitoring

*The **SFP Monitoring** tab allows to view details on optical fiber connectivity between modules (master system module, radio modules and extension system module). Optical interface diagnostic data is read from SFP connectors. The SFP Monitoring test is supported by the FSMF modules and onwards.*

Access to **SFP Monitoring** view: **Diagnostic ► SFP Monitoring**

An SFP (Small Form-factor Pluggable) is a physically compact connector design that consists of a housing fitted on a host board and a pluggable transceiver. It is developed for use in high-speed data transfer, including both copper-based and fiber-optic systems.

SFP Monitoring tab shows current (real-time) information about the connection between radio modules and system modules in current configuration. Selecting any of the listed SFPs displays further information in the **Details** panel.

8.8 Antenna Line Online Monitoring

This tab allows to monitor online antenna line characteristics

Access to **Antenna Line Online Monitoring** view: **Diagnostic ► Antenna Line Online Monitoring**

The **Antenna Line Online Monitoring** view allows the operator to monitor online antenna line characteristics such as:

- The values of Voltage Standing Wave Ratio (VSWR) for the Tx-capable antenna lines
- The values of Received Total Wideband Power (RWTP) for LTE and WCDMA
- the values of Received Signal Strength Indicator (RSSI) for GSM

To start monitoring, select the antenna line and click the **Start** button. The **Stop** button stops the monitoring. The obtained results can be exported to a CSV file.

8.9 RF Monitoring

> *This view allows to monitor the spectrum in order to detect radio frequency interference (RFI) and radio disturbance in the peripheral radio frequency (RF) path*

Access to **RF Monitoring**: **Diagnostic ► RF Monitoring**

Tests available in the **RF Monitoring** view:

- PIM Desensitization
- Distance to PIM (DTP)
- RF Scan

8.9.1 PIM Desensitization

> *This tab allows to perform PIM Desensitization tests.*

Access to **PIM Desensitization**: **Diagnostic ► RF Monitoring ► PIM Desensitization**

Passive Intermodulation Distortion (PIM) Desensitization is a test that verifies if PIM has any impact on the uplink channel for a particular antenna. To perform the test it is necessary to specify which antenna is to be tested. The following information on test configuration is displayed:

- Local cell
- Frequency band
- Bandwidth
- Frequency/EARFCN
- Power

The BTS configuration used for the test can be exported into ZIP file. Use the **Start** button to launch the test. The test results are saved to a local drive. For detailed instructions on viewing the test results, see Viewing RF monitoring results.

8.9.2 Distance to PIM (DTP)

> *This tab allows to perform Distance to PIM (DTP) test*

Access to **Distance to PIM (DTP)**: **Diagnostic ► RF Monitoring ► Distance to PIM (DTP)**

Distance to Passive Intermodulation Distortion (DTP) is a test that helps localize the actual place where Passive Intermodulation Distortion (PIM) is happening on an antenna line. To perform the test it is necessary to specify which antenna is to be tested. It is possible to configure additional test settings:

- Velocity factor
- Cable length

The following information on test configuration is displayed:

- Local cell
- Power

Use the **Start** button to launch the test. The test results are saved to a local drive. For detailed instructions on viewing the test results, see Viewing RF monitoring results.

8.9.3 RF Scan

This tab allows to perform RF scanning.

Access to **RF Scan**: **Diagnostic ► RF Monitoring ► RF Scan**

In this tab it is possible to trigger a scan to detect radio frequency (RF) interference. There are several attributes that must be configured to perform a scan:

- Antenna
- Capture type
- Local cell

Use the **Start** button to launch the test. The test results are saved to a local drive. For detailed instructions on viewing the test results, see Viewing RF monitoring results.

8.10 Test Models

*The **Test Models** views allow running downlink and uplink test models for each cell*

Access to **Test Models**: **Diagnostic ► Test Models**

The **Test Models** views allow running downlink and uplink test models for LTE cells.

The tests are available only if the BTS is in `Test Dedicated State`.

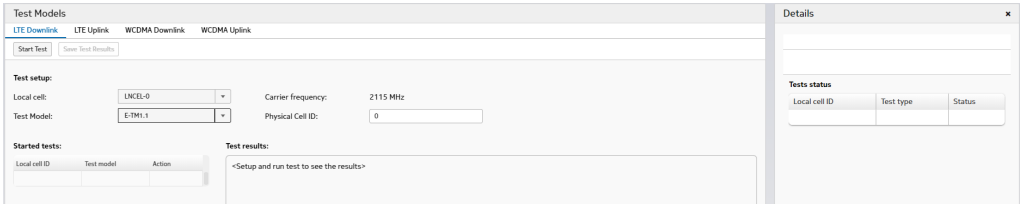
8.10.1 LTE Downlink

*The **LTE Downlink** tab allows to perform LTE downlink tests*

Access to **LTE Downlink**: **Diagnostic ► Test Models ► LTE Downlink**

To perform a test, select the cells for each test, as well as the test model and the physical cell ID. Clicking **Start** begins the test, and **Stop** stops the test. The results are displayed for each cell and can be saved to a file. The **Details** panel presents the status of each started test.

Figure 42 **LTE Downlink** tab view



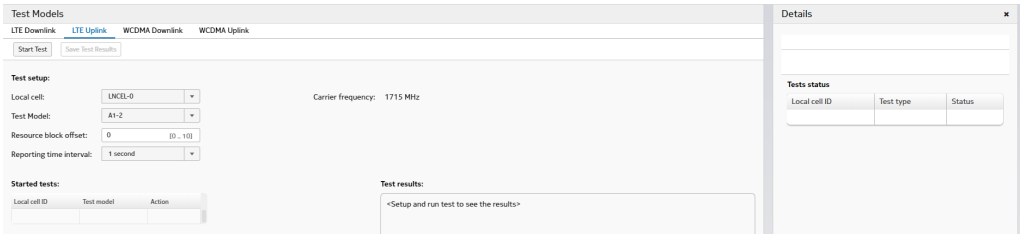
8.10.2 LTE Uplink

*The **LTE Uplink** tab allows to perform LTE uplink tests*

Access to **LTE Uplink**: **Diagnostic ► Test Models ► LTE Uplink**

To perform a test, select cells for each test, as well as the test model, reporting time interval and resource block offset. Clicking **Start** begins the test, and **Stop** stops the test. The results are displayed for each cell and can be saved to a file. The **Details** panel presents the status of each started test.

Figure 43 **LTE Uplink** tab view



8.11 Terminal

***Terminal** view description*

Access to **Terminal** view: **Diagnostic ► Terminal**

Terminal is the text console allowing the user to execute text commands. The **Terminal** output is cleared on each reload or view change. It is possible to save the output to a TXT file by using the `output-to-file` command. Using the `help` command lists all the available commands, while using the `help <command>` displays help information on the given command. Press the **Tab** key while typing a command to autocomplete it.

8.12 Snapshot

*The **Snapshot** tab is used to save the BTS snapshot.*

Access to **Snapshot** view: **Diagnostic ► Snapshot**

Snapshot is a functionality that can be used for troubleshooting and training purposes, in order to troubleshoot a problem with the site or to simulate a BTS site for training purposes. The snapshot file can be saved in connected mode and it contains the current status of elements, such as: used HW configuration, logs, alarms, HW and SW version information. Unlike the IMS2 file, the snapshot contains only the latest information, without the history.

The **Snapshot** view allows to download technical log files from the BTS. This tab contains a **Collect snapshot** button and snapshot collection settings. The snapshot collection settings allow to:

- Select LTE cells.
- Select snapshot coverage - all log files or the most important log files.
- Select target location - local or remote.
- Input filter keyword (optional).
- Include a reason for a report (optional).

Statuses of downloaded files are visible in the table at the bottom of the site. In order to cancel a technical report procedure, press the **Cancel** button. When the file collection is completed, the snapshot is saved in the selected location.

For more information on taking snapshots, see Taking snapshots with WebEM.

8.13 Reset to Test Dedicated State

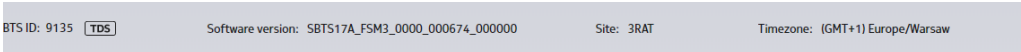
> ***Reset to Test Dedicated State*** *sets the site to a test dedicated state in order to perform tests.*

Access to **Reset to Test Dedicated State** view: **Diagnostic ► Reset to Test Dedicated State**

To perform tests such as LTE Uplink, LTE Downlink, WCDMA Uplink and WCDMA Downlink, the **Execute** procedure must be run first. It causes the site to reset to the `Test Dedicated State`. While in the `Test Dedicated State`, the site is treated as `Blocked`.

While the site is in `Test Dedicated State`, the icon TDS is displayed in the BTS site information area.

Figure 44 BTS site information



To leave the `Test Dedicated State` reset the BTS.

8.14 TWAMP RTT Measurements

> *RTT Measurements allow to measure and supervise the IP network conditions through the mobile backhaul between the BTS and some other point.*

Access to **TWAMP RTT Measurements** view: **Diagnostic ► TWAMP ► TWAMP RTT Measurements**

The **RTT Measurements** tab allows to measure and supervise the IP network conditions through the mobile backhaul between the BTS and some other point. The Round Trip Time (RTT) measurement functionality provides TWAMP-light (Two-Way Active Measurement Protocol) measurements, as specified in the IETF RFC 5357. The purpose of the measurements is to have an estimation of the quality and performance of the IP-based mobile backhaul for each QoS class independently, indicated by DiffServ Code points.

The results of the measurements are available in this tab if the hardware supports the RTT measurements and if it is configured using **Commissioning Wizard** or **Parameter Editor**.

8.15 Ethernet Link OAM

This view gives user access to link monitoring, Remote Failure Indication (RFI) and loopback functionalities.

Access to **Ethernet Link OAM**: **Diagnostic ► Ethernet Link OAM**

Link Monitoring

WebEM shows information on:

- Latest Events
  - Event type
  - Event subtype
  - Event time
  - Event code
  - Source address
  - Destination address
- Event Statistics
  - Event Type
  - Last remote interval events
  - Total remote events
  - Total remote TLVs
- OAM/non-OAM Statistics
  - Number of recived OAM protocol data units (OAMPDUs)
  - Non-OAMPDUs frames transmitted
  - Non-OAMPDUs frames received

There are four types of link events defined in the standard for a degraded Ethernet connection:

- **Errored Symbol Period Event**
- **Errored Frame Event**
- **Errored Frame Period Event**
- **Errored Frame Second Summary Event**

Loopback

This function is used for testing purposes in which the remote peer loops all received non-OAM Protocol Data Units (non-OAMPDUs). If the loopback mode is activated and it does not receive a disable command, the BTS returns to the normal working state after a timeout is reached.

The loopback testing is used for:

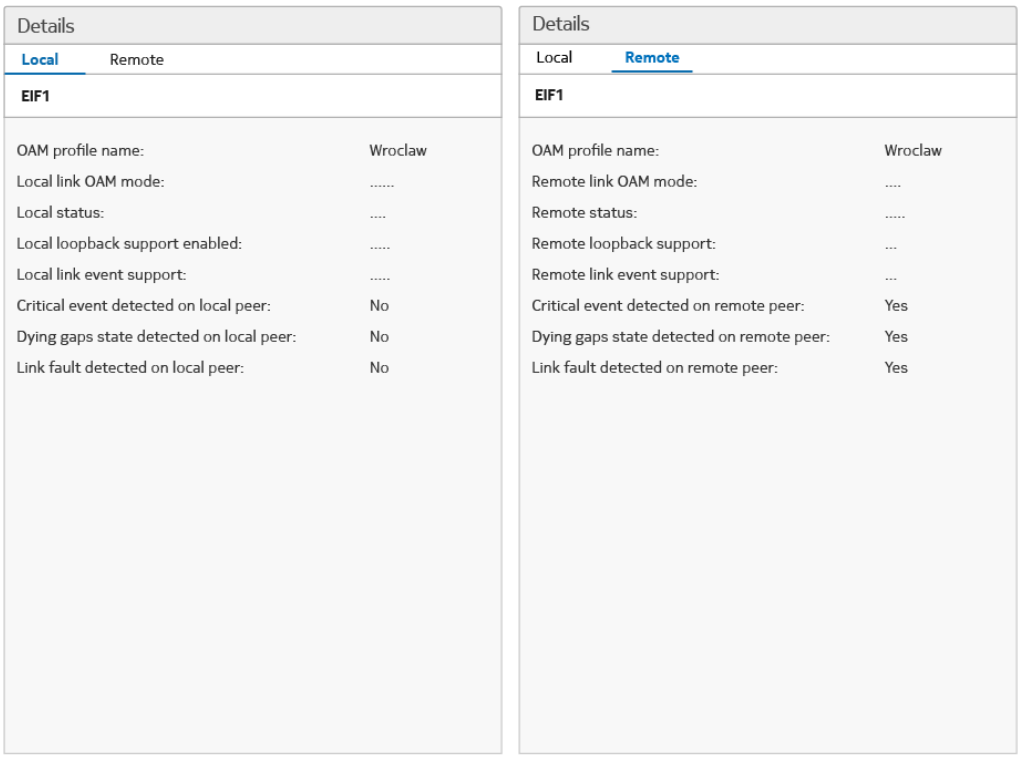
- Checking if the traffic is correctly sent and looped back to the local node.
- Checking statistics (errored frames).
- Identifying erroneous packets and packet drops in the link.
-

Note: Loopback mode interrupts the regular traffic, therefore it is recommended to use it for offline testing or only if all alternatives for online testing are exhausted.

Remote Failure Indication (RFI)

To check if there are any **Critical Link Events** detected, open the **Details** panel in the **Ethernet Link OAM** window.

Figure 45 Checking critical link events



8.16 Ethernet Service OAM

This view provides information on Ethernet Continuity Check, Remote Defect Indication (RDI). Loopback and Link Trace

Access to **Ethernet Service OAM**: **Diagnostic ► Ethernet Service OAM**

The Maintenance Association Endpoint (MEP) sends `Ethernet Continuity Check Messages` (Eth-CCMs) to its MEP peers according to the configured period. The MEP expects Eth-CCMs from every MEP peer.The Eth-CCM reports continuity loss, or unintended connectivity between MEPs. WebEM returns data such as:

- ID

- Mac address (static)
- Mac address (from remote MEP)
- Out of sequence CCM
- CCM reception
- CCM period
- Last RDI

Ethernet Link Trace retrieves information about the relationships between neighboring MEPs or Maintenance Association Intermediate Points (MIPs). It allows the detection of the number of S-OAM aware hops between two MEPs.

Ethernet Loopback verifies bidirectional connectivity between two peer MEPs, or between an MEP and an MIP.

To start the **Loopback** or **Link Trace**, click the corresponding button in the **Action** column.

8.17 IP Routing

*The **IP Routing** view allows to display information about static routes, routing policies and so on*

8.17.1 IPv4/IPv6 Routing

*A short description of the **IPv4/IPv6 Routing** views*

Access to **IPv4 Routing** view: **Diagnostic ► IP Routing ► IPv4 Routing**

Access to **IPv6 Routing** view: **Diagnostic ► IP Routing ► IPv6 Routing**

This tab provides information about static routes and forwarding tables for selected routing tables. The data is presented using two tables: **Static routes** and **Forwarding table**.

Information provided by **Static routes** table:

- Destination
- Prefix length
- Preferred source
- Gateway
- Preference
- IP MTU
- Trigger ID
- Trigger state

Information provided by **Forwarding table**:

- Type
- Destination
- Prefix length

- Gateway
- IP interface reference
- Preferred source
- Preference
- IP MTU
- Trigger ID

The **Change Static Routes** button redirects the user to the object class in **Parameter Editor** responsible for static route configuration.

8.17.2 Routing Policies

*A short description of the **Routing Policies** views*

Access to **Routing Policies** view: **Diagnostic ► IP Routing ► Routing Policies**

This view provides the following information about routing policies:

- Order number
- Reference to routing table
- Source IP address
- Source IP prefix length

The **Change Routing Policies** button redirects the user to the object class in **Parameter Editor** responsible for routing policy configuration.

Note: The policy order number of any new or old policy cannot be changed to an existing policy order number.

8.18 IP Security Associations

*A short description of the **IP Security Associations** views*

Access to **IP Security Associations** view: **Diagnostic ► IP Security Associations**

The **IP Security Associations** view provides information on:

- Internet Key Exchange (IKE) associations
  - Policy order number
  - IKE request ID
  - Local tunnel endpoint
  - Remote tunnel endpoint
  - Status
  - Mode
- Overall status of IKE associations
- Association information

- Policy order number
- Association request ID
- Local IP address
- Remote IP address
- Peer state
- Inbound security policy index (SPI)
- Outbound SPI

The displayed data can be filtered by **Policy order number**.

8.19 PMTU Discovery

In this view the on-demand path maximum transmission unit (PMTU) discovery can be performed.

Access to **PMTU Discovery**: **Diagnostic ► PMTU Discovery**

To start the test, insert the **Source IP address**, **Destination IP address** and **DSCP**. In return WebEM displays **Path Maximum Transmission Unit** and **Local Maximum Transmission Unit**.

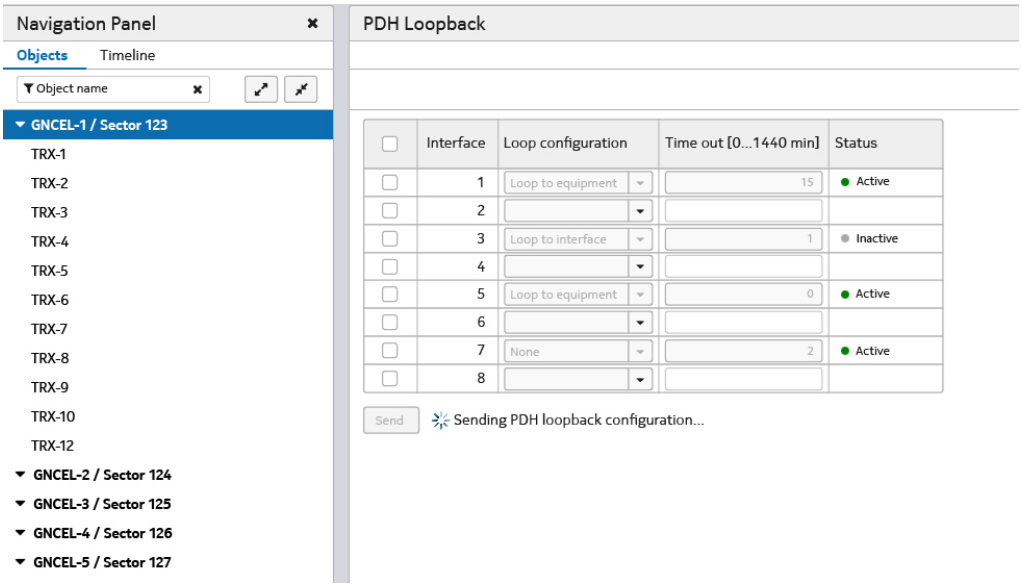
8.20 PDH Loopback

This tab allows to perform PDH Loopback

Access to **PDH Loopback**: **Diagnostic ► PDH Loopback**

To enable the **PDH Loopback** function select the Interface and Loop configuration and then click **Send**. Additionally, it is possible to set the **time out**.

Figure 46 PDH Loopback



9 Procedures tab

*The **Procedures** tab contains four tabs allowing to disable the Ethernet port, R&D service port or service account SSH, as well as execute procedures connected to autoconnection, changing the BTS RnD parameters and downloading the Info Model history.*

9.1 Calibrate EPIMC FHS

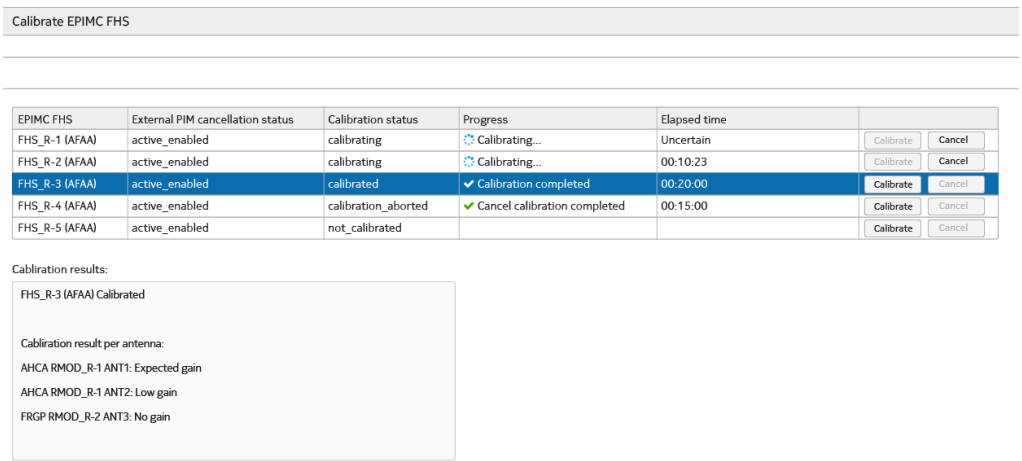
*The **Calibrate EPIMC FHS** tab allows to calibrate passive intermodulation cancellation (PIMC) for a fronthaul switch.*

Acces to **Calibrate EPIMC FHS**: **Procedures ► Calibrate EPIMC FHS**

The passive intermodulation cancellation (PIMC) functionality is based on the PIMC engine. The hardware and software of the engine monitor the downlink signals coming from the Nokia AirScale system module and compute a PIM model in real time. The PIMC engine intercepts the uplink signals coming from radio modules, synchronizes any PIM interference using the PIM model, and subtracts the PIM noise or interference according to the identified model. This reduces the uplink PIM interference and a cleaner signal is sent to the system module.

In order for this functionality to work properly, calibration is required. To perform calibration, click the respective button next to the fronthaul switch (FHS). Calibration results are shown as in the Figure 47: Calibrate EPIMC FHS

Figure 47 Calibrate EPIMC FHS



9.2 Ethernet Port Security

*The **Ethernet Port Security** panel allows to disable or enable an Ethernet port.*

Access to **Ethernet port security** view: **Procedures ► Ethernet port security**

The security for the Ethernet port feature is enabled by default. If the feature is enabled, the sensitive internal traffic is separated from external traffic. The status can be changed by using the **Disable** button. There is also an option to save the configuration in the network plan. To do so, mark this option before changing the status.

9.3 RnD Service Port

*The **R&D Service Port** panel allows to disable or enable an R&D service port.*

Access to **R&D Service Port** view: **Procedures ► R&D Service Port**

The R&D service port is enabled by default. The status can be changed by using the **Disable** button. There is also an option to save the configuration in the network plan. To do so, mark this option before changing the status.

9.4 Service Account SSH

*The **Service Account SSH** panel allows to disable or enable the Service Account Secure Shell (SSH).*

Access to **Service Account SSH** view: **Procedures ► Service Account SSH**

The Service Account SSH is enabled by default. The status can be changed by using the **Disable** button. There is also an option to save the configuration in the network plan. To do so, mark this option before changing the status.

9.5 Change BTS RnD Parameters

*The **Change BTS R&D Parameters** tab allows to edit the BTS R&D parameters.*

Access to **Change BTS R&D Parameters**: **Procedures ► Change BTS R&D Parameters**

The **Change BTS R&D Parameters** tab allows to set the following components:

- Index of SwSystem component
- R&D setting type:
  - Factory defaults
  - Dynamic changes
  - Persistent changes
  - Persistent over one reset changes
- R&D parameters in JSON format

9.6 IM Snapshot

*The **IM Snapshot** tab allows to download IM snapshots.*

Access to **IM Snapshot**: **Procedures ► IM Snapshot**

The **IM Snapshot** tab contains the **Execute** button. Clicking this button starts the IM snapshot download procedure. The location where the file is saved depends on the browser settings.

9.7 BTS Log Level

In BTS Log Level view, the operator can change the level of collected BTS logs.

Access to **BTS Log Level**: **Procedures ► BTS Log Level**

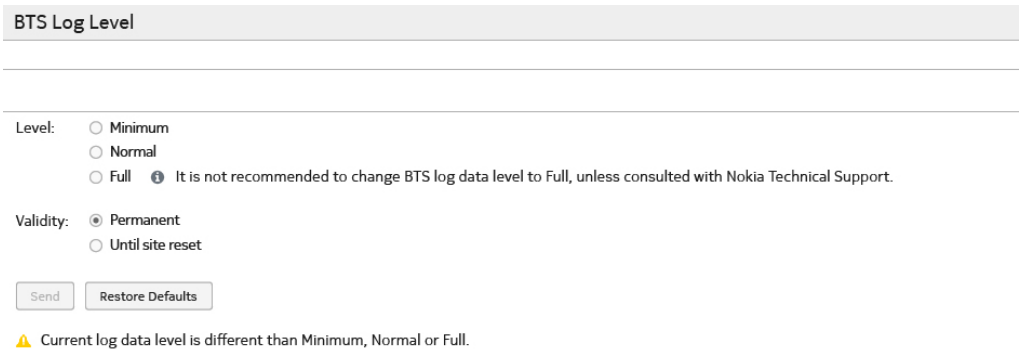
The BTS logs are a part of the collected snapshot data. This tab allows to adjust a level of the saved data. The operator can choose minimum, normal or full level of logs.

More detailed logs are chosen for troubleshooting purposes. When there are no problems, less detailed logs save space on the BTS.

Note: Before using full the BTS log level, contact Nokia Technical Support.

In this view the user can determine if the chosen BTS log level is valid permanently or until the site reset.

Figure 48 BTS Log Level view



10 Instructions

This section provides a list of step-by-step instructions on how to perform the most common BTS-related activities (such as commissioning, SW update, parameter editing, running diagnostics) using WebEM.

10.1 Launching the WebEM tool

The WebEM tool can be launched in several different ways, both with and without a connection to the BTS.

10.1.1 Launching the WebEM tool when connected to the BTS (online)

When a user's PC is connected to the BTS via a remote or local BTS port, the WebEM tool can be started directly in the web browser.

Procedure

1 Start the browser.

Chrome is a recommended browser.

2 Type the BTS IP address.

The IP address must be the M-plane address of the BTS, or (if locally connected) the LMP address. A connection using this address is possible only when the BTS is correctly configured.

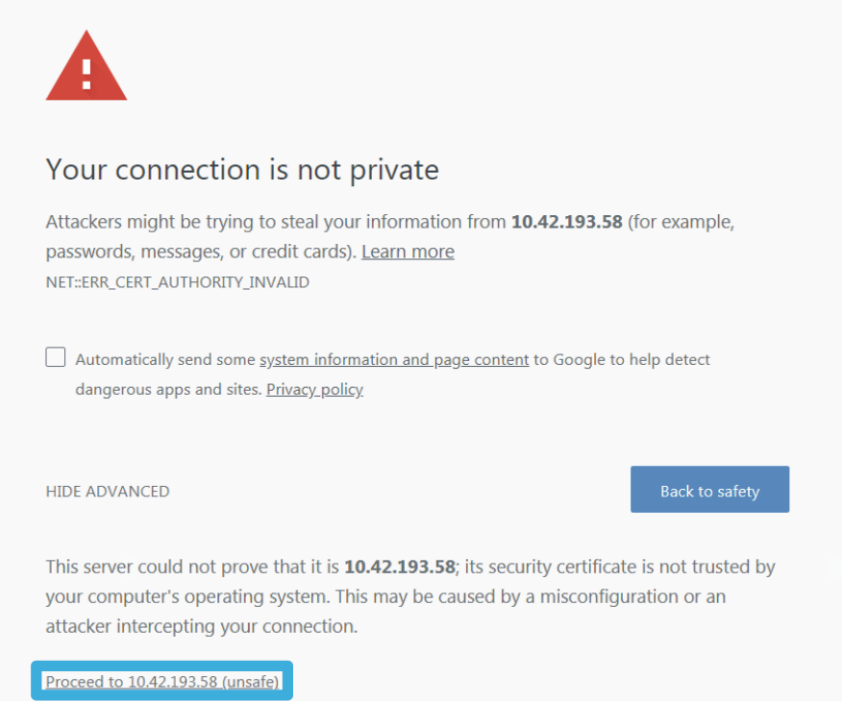
Note: The M-plane address is specific to the BTS. LMP addresses used for local connection:

- For the primary core: `https://192.168.255.129`
- For the secondary core: `https://192.168.255.119`

3 Solve the certificate issue (optional).

In case the BTS certificate is changed, the browser may fail to validate the SSL certificate. Click **Proceed to [localhost] (unsafe)** to solve this issue.

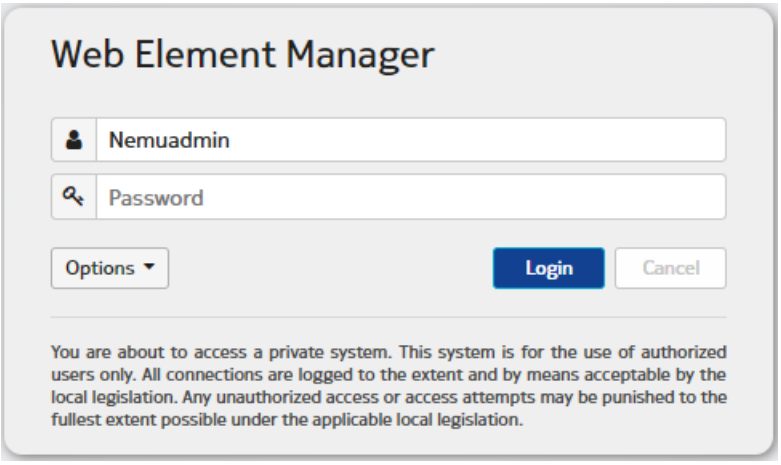
Figure 49 Solving the certificate issue



4 Log in to the web browser using local account credentials or Centralized User Accounts.

Step example

Figure 50 Login to WebEM



The default credentials are:

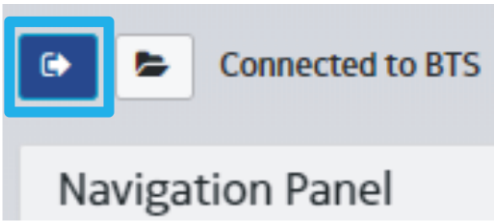
- Username: Nemuadmin
- Password: nemuuser

It is recommended to change the default credentials.

5 If WebEM is not automatically connected, click the **Connect** button.

Step example

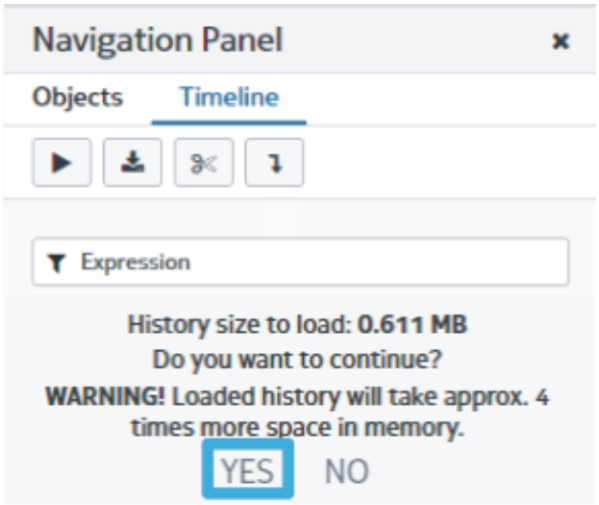
Figure 51 Connecting to the BTS



Result

The connection to the BTS is established, and information related to the site is displayed. During the connection, it is possible to download a history of events that occurred a limited time before the connection was established, by using the download history option.

Figure 52 Downloading history



10.1.2 Launching the WebEM tool offline

It is possible to launch the WebEM tool offline. This option is useful when viewing IMS2 files from different BTSs.

Before you start

Launching the WebEM tool offline is performed using the HTML file. YThis file can be downloaded when the WebEM tool is launched using an online BTS (see Launching the WebEM tool when connected to the BTS (online)). When the WebEM tool is running in the Chrome browser, click **CTRL+S** or **Mouse Right Click+Save as...** to save the HTML

file. WebEM offline is not connected to the BTS. WebEM offline can be used, for example, to prepare site configuration, save it, and later, when connected to the BTS, send it to the BTS.

To view the IMS2 file or snapshot in WebEM, proceed with the following:

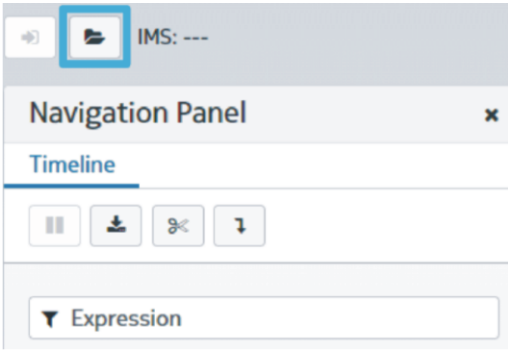
Procedure

1 Launch previously saved HTML file in the Chrome browser.

2 Click **Open ims2 file**.

Step example

Figure 53 **Open ims2 file** button



3 Navigate to the IMS2 or snapshot file and click Open.

10.1.3 Launching and authenticating WebEM from a third-party application

Instructions on how to launch WebEM from a third-party application

Procedure

1 Generate a token.

To generate token, send an HTTP_POST request with the username and password: `{“username”:”<<User Name>>”,”password”:”<<password>>”}`.

Step example

An application that can be used to send an HTTP_POST request is **cURL**.

In this application, use the command: `curl https://btsAddress:443/NetActSSO/token -X POST -H Content-Type:application/json -d "{\"username\":\"UserName\",\"password\":\"pass\"}" -k`, where `btsAddress` is an M-plane BTS address, `UserName` is a user name and **pass** is a password.

Step result

The token is generated and the user receives the following object: `{token:"<<TOKEN>>"}`, for example `{"token" : "46f4db42-ed1d-4530-b46d-9eced6220e02"}`.

2 Open Google Chrome.

3 Add flags to Chrome to automatically skip the warning about certificate incompatibility (optional).

Note: For automation purposes, it is possible to run the Google Chrome application from a command line interface, if it is added to PATH then execute: `chrome --new-window`

To skip the warning about certificate incompatibility automatically, add additional flags: `--ignore-certificate-errors --test-type`

Keep in mind that these are Google Chrome specific flags and might not be supported in other browsers.

4 In the browser bar insert the URL: *`https://btsAddress/?token=<<TOKEN>>`*

Step example

`https://10.11.12.13/?token=46f4db42-ed1d-4530-b46d-9eced6220e02`

10.2 Recommended way of refreshing the running WebEM session

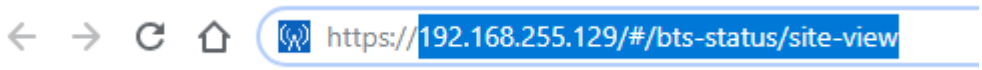
In case of WebEM, refreshing the browser with the F5 button will result in clearing the web browser's cache, which breaks optimizations made in the WebEM tool - web browser must execute more requests to SBTS causing more delays and data transfers.

Procedure

1 Enter WebEM address again instead of clickingF5 button.

2 The operator should remove everything after # (including # itself) from the address and press Enter.

Figure 54 Modifying the address in the web browser



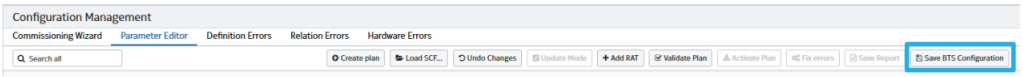
10.3 Saving site configuration file (SCF)

Instructions on how to save a site configuration file.

Procedure

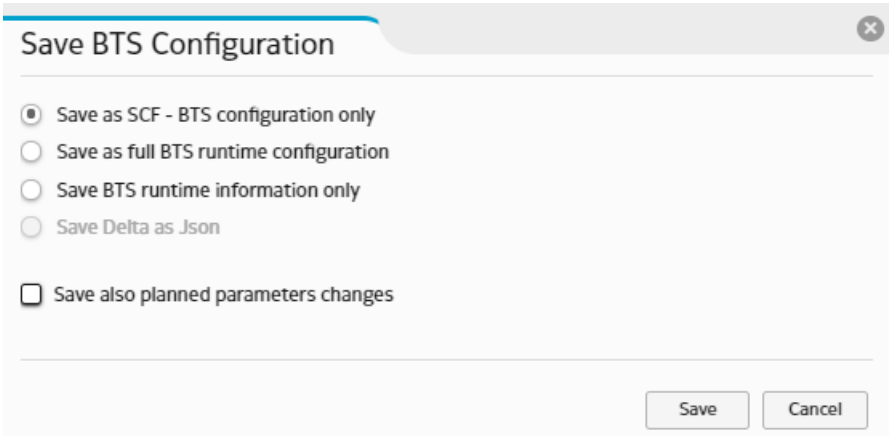
1 Go to **Configuration ► Configuration Management ► Parameter Editor** view.

2 Use the **Save BTS configuration** button.



3 Select the required variant and click **Save**.

Figure 55 Saving the BTS configuration



Note: In case of saving before activation of changed parameters, check **Save also planned parameters changes** to include the planned changes of parameters in the backup.

10.4 Taking snapshots with WebEM

Snapshots enable capturing the state of an SBTS at a particular point in time.

Purpose

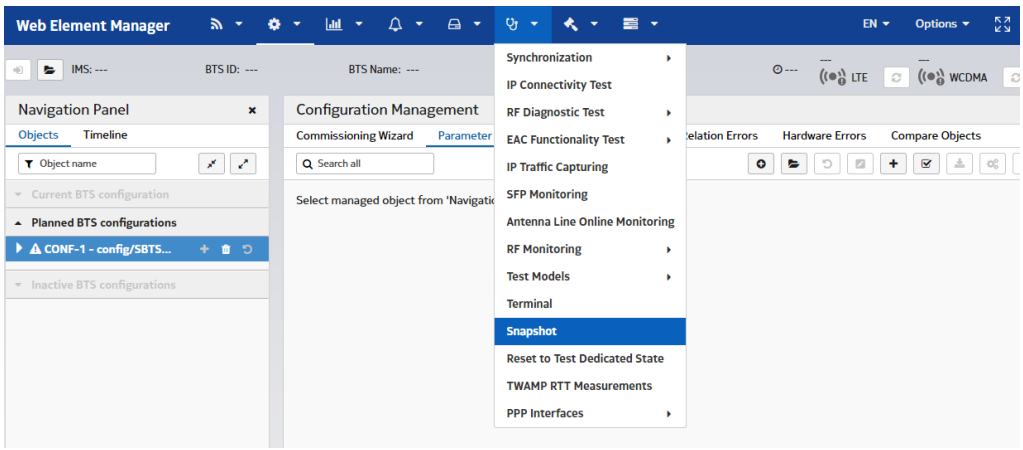
For troubleshooting and fault traceability of the SBTS.

Procedure

1 Open **WebEM** and go to **Diagnostic ► Snapshot**.

Step example

Figure 56 Selecting Snapshot

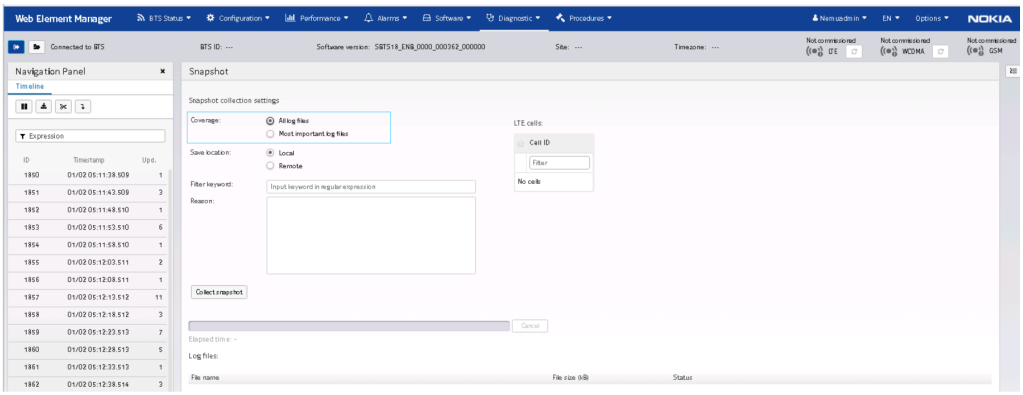


2 For **Coverage** select either **All log files** or **Most important log files**.

The **All log files** snapshot coverage includes all the files while **Most important log files** snapshot coverage includes only the most important files in the technical log.

Step example

Figure 57 Selecting snapshot coverage



3 **Select target location** to be **Local** or **Remote**.

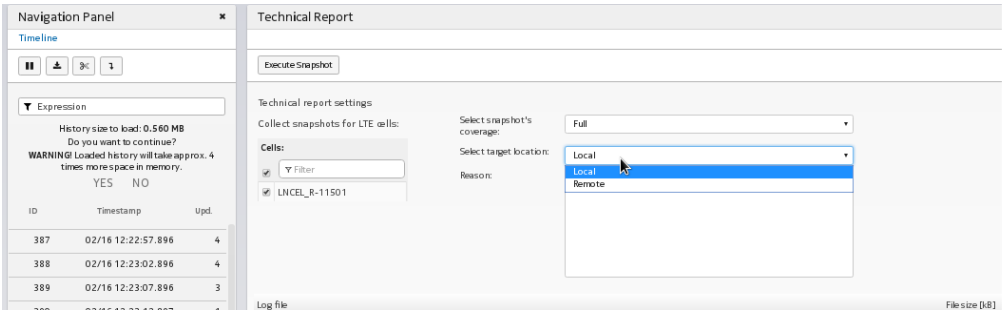
Select target location with one of the options given below:

- Local drive: Create a snapshot and place it on the SBTS and download a copy to a local drive.
- Server: Create a snapshot and place it on the SBTS and save a copy to an external server.

Note: In case the target location is set to **remote**, make sure that the `Diagnsostic Snapshot destination (diagSnapDestination)` parameter is configured. If the parameter value is **lss**, configure the parameters under the `Local symptoms server configuration (lssConfig)` structure as well. To configure these parameters go to **Configuration ► Configuration Management ► Parameter Editor**. Use the search box to find the required parameters.

Step example

Figure 58 Selecting the target location

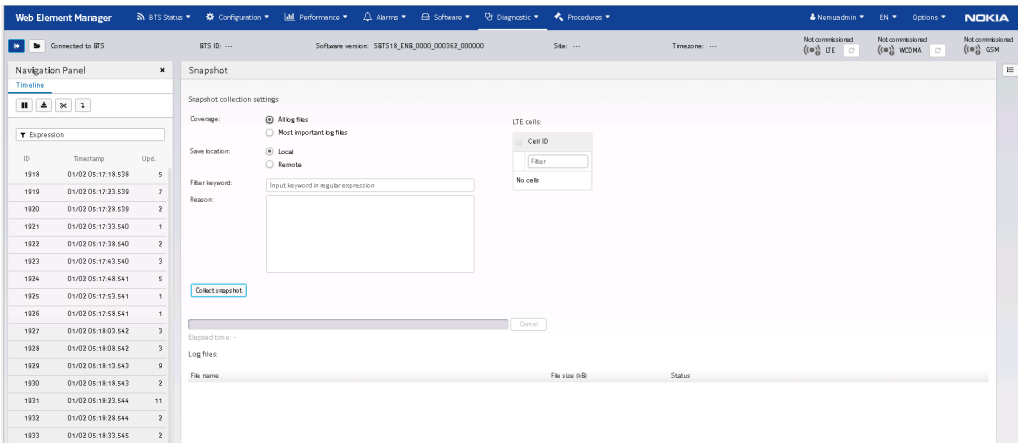


In case of dual-core configuration:

- The technical logs related to the primary and secondary system modules and related resources (BBMODs, RMODs, ALDs, cells and more) are collected and saved in the technical report.
- If the connection between the two system modules is broken, connect to the secondary system module using LMP to collect technical logs from the secondary system module and related resources. Then connect to the primary system module using LMP to collect technical logs from the primary system module and related resources.

4 Click **Collect snapshot**.

Figure 59 Collect snapshot



Note: To stop the process during snapshot collection, click **Cancel**.

10.5 Saving an IMS2 file

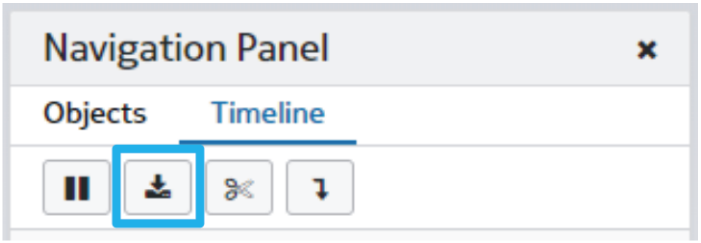
The InfoModel snapshot file (IMS2) is mainly used for BTS troubleshooting purposes and contains a full BTS state snapshot. The IMS2 file can be loaded to WebEM to view the BTS state and its configuration the same way as via an actual connection to the BTS. The InfoModel snapshot contains full BTS runtime data for a certain period of time, making it possible to analyze BTS behavior during that period. READ

Procedure

1 Select the **Timeline** tab from the **Navigation Panel**.

2 Click the **Save IMS2** button.

Figure 60 Saving the IMS2 file



10.6 Running TRS diagnostics

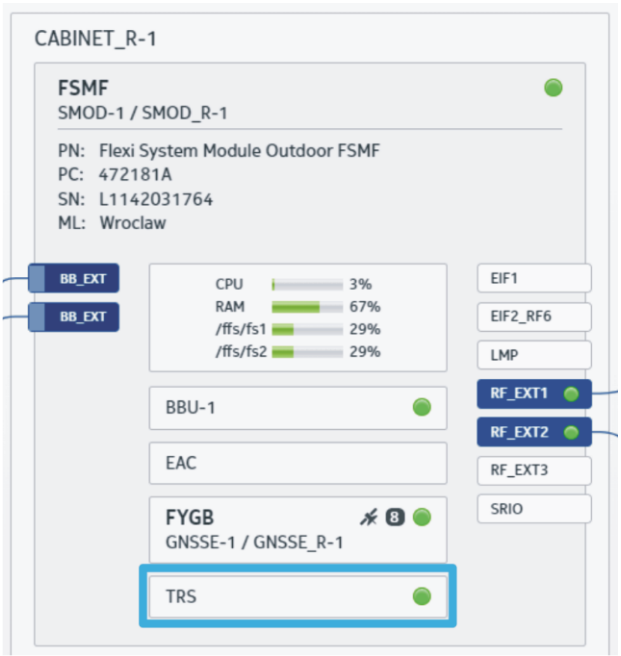
*The TRS diagnostics view is available for transport units selected in **Site Runtime View**.*

Procedure

1 Go to **BTS Status ► Runtime View ► Site Runtime View**.

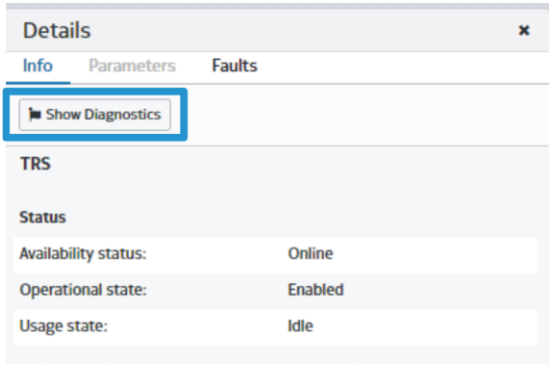
2 Select the transport (TRS) module.

Figure 61 Selecting TRS module



3 Click on the **Show Diagnostics** option in the **Details** panel.

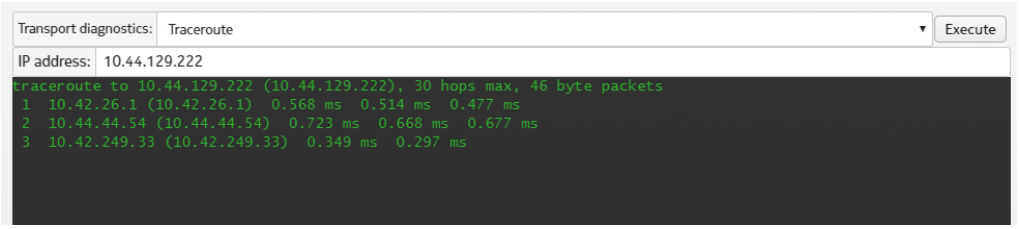
Figure 62 **Show Diagnostics** in the **Details** panel



4 Select the desired test from the list and click **Execute** to run it.

Some tests require some input data (like IP address) before executing. The results of the test are displayed on the screen. Note that selecting any other test or switching the views loses the results.

Figure 63 Traceroute test result example



10.7 Viewing RF monitoring results

The RF monitoring tests are executed using WebEM, however the results can be visualized using a standalone, separate tool called RF monitor.

Before you start

The **RF Monitor** tool is available together with the BTS software, and requires an installation on the user's PC. It is launched in a web browser, similarly to WebEM. Before launching **RF Monitor**, make sure that to have **MatLab Runtime R2015a** installed (in the same version, 32-bit or 64-bit, as the RF monitor). It can be downloaded from: **https://www.mathworks.com/products/compiler/matlab-runtime.html**

Procedure

1 Start RF Monitor using the desktop shortcut.

Step result

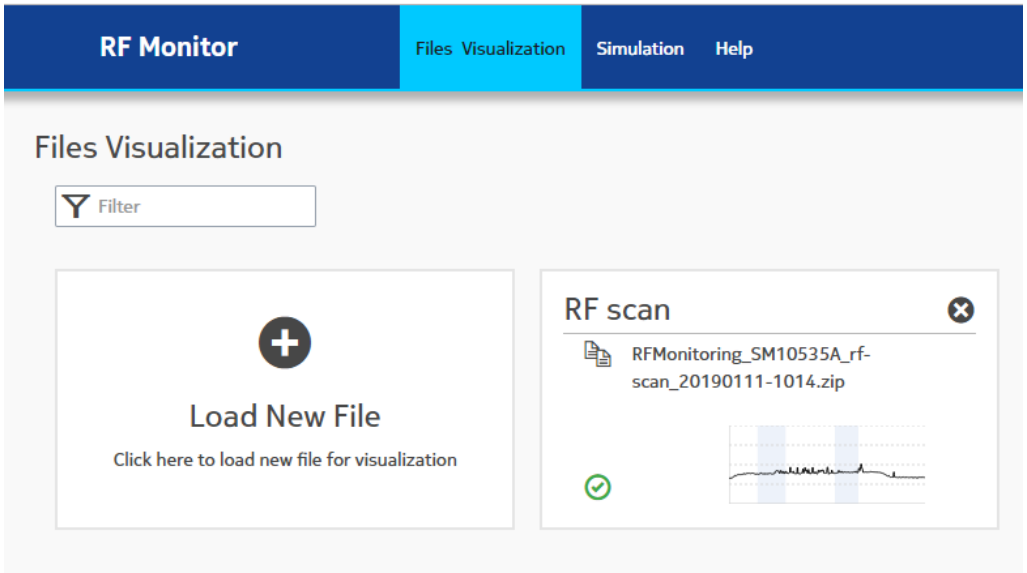
A notification informs that RF monitoring is starting, and a new web browser page opens. If that does not happen, type `http://localhost:8090` in the browser to launch RF Monitor manually.

2 Load the RF monitoring test result using **Load New File**.

The files must first be generated by the WebEM RF monitoring functionality. It is possible to load several files.

Step result

Figure 64 RF Monitor

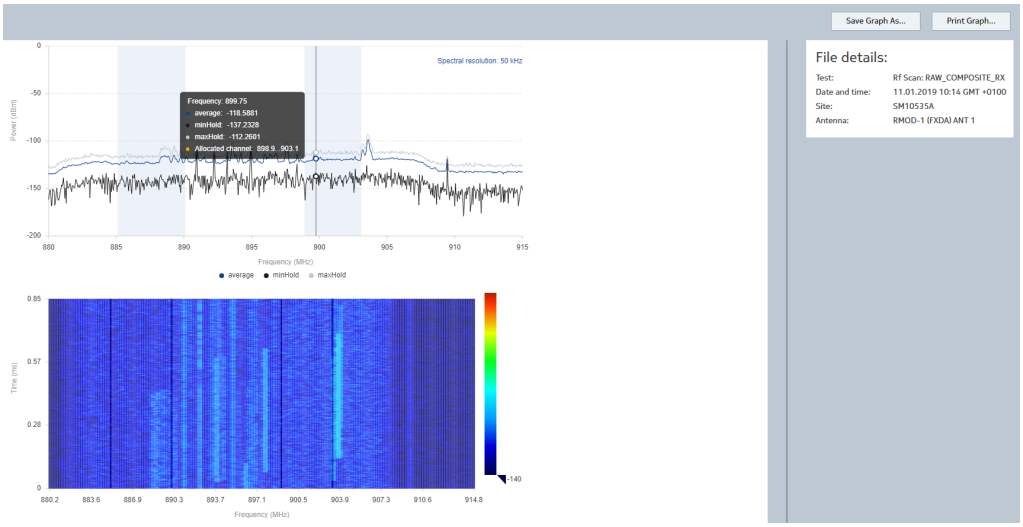


3 Click on a visualisation result to see them.

Step result

The test results are presented in an interactive, graphical form. It is also possible to save or print the graph.

Figure 65 Test results representation



11 Frequently asked questions about WebEM

Web Element Manager resembles ADMIN tool, is it the same application?

Web Element Manager is an evolution of ADMIN tool that was delivered in release LTE 16A. Starting from release LTE 19/SRAN 17A Web Element Manager has been enhanced with parity to BTS Site Manager and became the official Element Manager.

Will BTS Site Manager be available in releases LTE19 and onwards?

No. Web Element Manager is the only Element Manager to be used.

ADMIN tool has been accessible over port 3600. Is Web Element Manager to be accessible in the same way?

Starting from release LTE19/SRAN 17A, Web Element Manager is deployed on default HTTPS port, 443. Modern browsers do not require the user to provide port whenever referring to the default port, so it is possible to open both **https://mplaneIpOrLmpIp:443** or just **https://mplaneIpOrLmpIp**.

How to log in to Web Element Manager?

To log in to Web Element Manager, use the same credentials that were used before to log in to BTS Site Manager.

Is the communication between Web Element Manager and BTS secure?

Yes. Web Element Manager uses HTTPS (Hypertext Transfer Protocol Secure) and WSS (Web Socket Secure).

What will happen if more than one user wants to execute the same operation at the same time?

In practice, a request comes to the BTS first and it gets executed while the other requests get rejected. The user is notified about the fact that their request has been rejected. However, no additional info with the reason for rejection is to be provided.

Is it possible to log in to the application with read-only access?

Yes. There is a dedicated account profile, that must be first activated via account management view, which has read-only access. In addition to it, it is possible to manually downgrade own privileges during the login process by selecting an adequate flag.

What access levels are currently supported?

Currently, there are four different access levels supported: BTS Read Only User, BTS Application Administrator, BTS Security Administrator, and BTS System Administrator.

Is it possible to communicate with other connected users?

No. There is no “chat” functionality implemented in the Web Element Manager. However, it is possible to browse the list of already connected users in a dedicated view (Sessions List).

Are actions triggered by Element Manager atomic?

Yes. For example, even if during the recommissioning procedure multiple objects are being edited the whole procedure is atomic.

Is it possible to dump configuration from given timestamp?

Yes, simply select given timestamp in timeline component (the left side panel of application), go to Parameter Editor and save the configuration from there. Please note that only one timeframe can be selected at the same time. If anything is selected in the timeline panel , then the latest configuration will be exported.

Is it possible to show the current number of active data sessions and VoLTE calls?

In WebEM GUI and in WebEM Remote Tool user can check an average number of active UEs per cell during the measurement period (15 minutes by default). A UE is considered as active if at least a single non-GBR DRB has been successfully configured for it. The same value can be obtained by checking the value of `CELL_LOAD_ACTIVE_UE_AVG` counter (`M8051C57`)

Does RUEM log contain login reference of the user that triggered operation?

Yes, it does.

Is it possible to export historical changes from application to check the state of BTS offline?

Yes. It is possible either via “Save ims2” button on the timeline (changes fetched by WebEM during the session) or via IMSnapshot/Snapshot procedure (changes fetched by BTS itself starting from startup procedure).

Why Web Element Manager logs (ims2 file) size differ when it is saved by application or fetched by IM Snapshot / Snapshot procedure?

An ims2 file fetched from BTS is a compressed one.

Is it possible to check what was the state of the BTS prior to the connection?

Yes. Once the connection is established there is a pop-up window in the timeline component where the load history will be shown for all the prior connections.

Is the interface between Web Element Manager and BTS opened and published?

No. The interface between WebEM is binary, it is not intended to be used by 3rd parties. For automatization purposes, WebEM Remote Tool (former BTS CLI) should be used.

Is there a support for real-time counters?

Yes. Selected counters are reported in Real-time Measurement view.

Is validation mandatory for plan activation?

Yes. The validation phase is mandatory to trigger plan activation although its results might be explicitly skipped.

Where can I find Web Element Manager manual?

Web Element Manager manual is available in Discovery Center. It can also be downloaded from BTS, via the “Download Help” functionality in the application.

Is it possible to send the plan first and activate it later?

Yes. It is possible to send one plan/delta to BTS to activate it later. Please note that the newer plans/deltas overwrite the previous ones.

Is it possible to attach notes to plans, especially those intended to be activated later?

No. There is no such a functionality yet.

Does Web Element Manager support extracting GSM configuration file for LTE & GSM sharing feature?

Yes, it does.

Does Web Element Manager support possibility to check alarm history that happened in the past?

Yes, but indirectly. You have to first load history prior to the connection.

