

Keysight Open RAN Simulators, Cloud Edition 3.1

DuSIM

User Guide

Notices

Copyright Notice

© Keysight Technologies 2022–2024

No part of this document may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Keysight Technologies, Inc. as governed by United States and international copyright laws.

Warranty

The material contained in this document is provided “as is,” and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

U.S. Government Rights

The Software is “commercial computer software,” as defined by Federal Acquisition Regulation (“FAR”) 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement (“DFARS”) 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly,

Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at <http://www.keysight.com/find/sweula>. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Contacting Us

Keysight headquarters

1400 Fountaingrove Parkway
 Santa Rosa, CA 95403-1738
www.ixiacom.com/contact/info

Support

Global Support	+1 818 595 2599	support@ixiacom.com
<i>Regional and local support contacts:</i>		
APAC Support	+91 80 4939 6410	support@ixiacom.com
Australia	+61-742434942	support@ixiacom.com
EMEA Support	+40 21 301 5699	support-emea@ixiacom.com
Greater China Region	+400 898 0598	support-china@ixiacom.com
Hong Kong	+852-30084465	support@ixiacom.com
India Office	+91 80 4939 6410	support-india@ixiacom.com
Japan Head Office	+81 3 5326 1980	support-japan@ixiacom.com
Korea Office	+82 2 3461 0095	support-korea@ixiacom.com
Singapore Office	+65-6215-7700	support@ixiacom.com
Taiwan (local toll-free number)	00801856991	support@ixiacom.com

Table of Contents

Contacting Us	3
Chapter 1 DuSIM overview	9
DuSIM feature summary	10
Objectives-based testing	11
UI overview	12
Chapter 2 Initial administrator login	14
Chapter 3 User login and logout	17
Chapter 4 Build and run a test	18
Step 1: Create a new test config	19
Step 2: Configure Global Settings	21
Step 3: Establish connectivity with your DUT	22
Step 4: Configure DU-CP test nodes	23
Step 5: Configure DU-UP test nodes	25
Step 6: Assign agents to the CU test nodes	26
Step 7: Configure eNodeB node	29
Step 8: Configure CU-Simulated node	31
Step 9: Configure mobile device definitions	33
Step 10: Create Scenario Groups	34
Step 10.1: Add and manage Scenario Groups	35
Step 10.2: Configure mobility	36
Step 10.3: Create Test Suites	38
Step 10.4: Defining parallel procedures	40
Step 11: Configure UEs	42
Step 12: Start the test	43
Step 13: View real-time test results	44
Chapter 5 Global Settings	46

Access Global Settings	47
Technical Spec Version	48
DNS Settings	48
Advanced Settings	49
Impairment Settings	54
Session Settings	55
DNNs Settings	55
MMW Settings	56
TM Settings	57
CA Certificates Settings	57
Chapter 6 Assign and manage agents	58
About traffic agents	59
Assigning agents to nodes	60
Agent management	62
Network Management	65
Chapter 7 CU configuration settings	67
CUs panel	68
CU panel	68
F1-C Interface Settings	70
X2-C Interface Settings	70
Xn-C Interface Settings	71
F1-U Interface Settings	72
Chapter 8 DU-CP configuration settings	73
DU-CP Range panel	74
DU-CP RANGE panel	75
Cells settings	77
Measurement Timing Configuration	79
F1-CP Interface Settings	80
DU-PROCEDURE RANGE panel	86
Chapter 9 DU-UP configuration settings	88
DU-UP RANGES panel	89

DU-UP Range panel	90
Chapter 10 eNodeB configuration settings	96
eNodeB RANGES panel	97
eNodeB RANGE panel	98
Cells settings	99
X2-C Interface Settings	100
X2-U Interface Settings	105
S1-C Interface Settings	107
S1-U Interface Settings	112
Chapter 11 EPC configuration settings	114
MME Pools panel	115
MME panel	116
Chapter 12 CU-Simulated configuration settings	118
CU-Simulated Ranges panel	119
CU-Simulated Range panel	120
Node Settings	120
Cells Settings	121
Subscriber Settings	122
N2 Interface Settings	124
N3 Interface Settings	126
Xn-C Interface Settings	127
Xn-U Interface Settings	128
Chapter 13 5G-CORE configuration settings	131
Chapter 14 UE configuration settings	133
UE panel	135
UE RANGE settings	137
Identification settings	138
Subscriber SIM settings	139
Subscriber ESM settings	141
Subscriber EMM settings	143
Subscriber NR Provisioning	145

Subscribers DNN settings	146
Subscriber Network Slicing settings	147
UE Device settings	149
Chapter 15 UE Test Objective settings	151
User Plane panel	152
Stateless UDP Traffic	154
Data Traffic	155
Voice Traffic	158
Video OTT	163
DNS Client Traffic	164
UDG Traffic	166
Chapter 16 Scenario Group settings	170
Mobility settings	172
Test Suite settings	175
Test procedures for SA	176
Deregistration	177
PDU Session Establish	178
PDU Session Release	180
Registration	182
Service Request	183
Test procedures for NSA tests	184
Attach	185
Detach	186
ENDC Configuration Update	187
EPS Bearer Activation	188
EPS Bearer Deactivation	189
Inter eNB Handover	190
PDN Connection Activation	191
PDN Connection Deactivation	193
SCG Release	195
SGNB Addition	196

Test procedures for SA and NSA	198
Application Traffic	199
Delay	200
DU Initiated Release	201
NR-U Modification Request	202
Chapter 17 Manage and use test sessions	204
Save test sessions	205
Manage test sessions	206
Import and export sessions	210
Delete configs and sessions	212
Chapter 18 Manage DuSIM licenses	214
Licensing Requirements	215
License Manager	216
License server	218
Chapter 19 Manage DuSIM users	219
Chapter 20 DuSIM title bar settings	222
Chapter 21 Troubleshooting	225
View Notifications and Test Events	226
Collect Diagnostics	228
Index	229

CHAPTER 1

DuSIM overview

In the 5G New Radio (NR) transport architecture, the original LTE BBU functions are split into three parts: Central Unit (CU), Distributed Unit (DU), and Radio Unit (RU). The 3GPP *Higher Layer Split* (HLS) refers to the CU/DU split (over the F1 interface) and the CU-UP/CU-CP split (over the E1 interface).

Keysight DuSIM is a cloud-native gNB Distributed Unit (DU) simulator that provides comprehensive support for testing the performance and functionality of your gNB Central Units (CUs) in standalone (SA), non-standalone (NSA) and simulated-CU network topology. It simulates user plane and control plane traffic flowing over the F1 interface for SA mode and additionally S1 and X2 interface for NSA mode topology. Simulated-CU mode simulate Xn interface towards your gNB CU (the DUT) and it responds to traffic sent from your DUT to the simulated gNB DU.

Chapter contents:

DuSIM feature summary	10
Objectives-based testing	11
UI overview	12

DuSIM feature summary

DuSIM runs on top of the Keysight Open RAN Simulators Cloud Edition (ORAN SIM CE) infrastructure, a cloud-native platform that enables multiple Keysight ORAN SIM CE products (CuSIM, DuSIM, CoreSIM, and LoadCore) to run in parallel. This test solution provides seamless integration on the same infrastructure as the Device Under Test (DUT), sharing the same look-and-feel and functionality across all products. The Keysight ORAN SIM CE platform can accommodate various cloud types—public and private—via the deployment of containers or complete Virtual Machines (VMs).

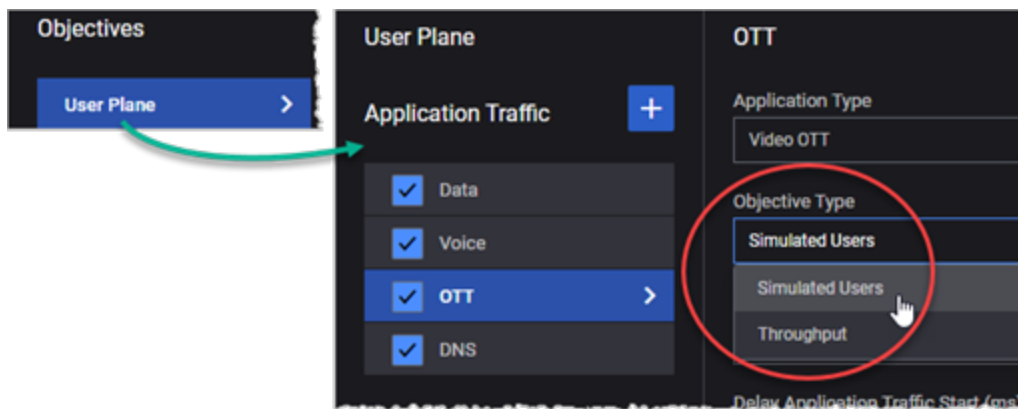
DuSIM feature summary:

- Supports testing in 5G SA, NSA, and simulated-CU networks.
- Features a web-based user interface (UI) through which you manage all aspects of your DuSIM testing environment, including test creation, execution, and management; traffic agent deployment and management; statistical results and reporting; and user and license administrative control.
- Traffic agents generate traffic over the F1-U/S1-U/X2-U/Xn-U (user plane) and F1-C/S1-C/X2-C/Xn-C (control plane) interfaces. The agents are implemented as containers or virtual machines, depending upon the platform on which they are deployed. The supported platforms include:
 - public clouds: Amazon Web Services (AWS)
 - private clouds: VMware ESXi 6.5 and ESXi 6.7
 - containers: Kubernetes with OpenShift, Flannel, and Calico
- The agents can be horizontally scaled to support a very high level of application traffic throughput and control plane procedure rates.
- Uses a proprietary goal seeking algorithm to evaluate key performance indicators (such as bandwidth and connections per second) to help you evaluate the real performance of the network infrastructure and device under test (gNB-CU).
- Supports multi-thread control plane process flows.
- Provides extensive control plane and user plan statistics coverage.
- Provides support for script-based impairments (Python scripts).
- Is based on a REST API.

Objectives-based testing

The Keysight proprietary goal seeking algorithm allows DuSIM test agents to converge towards stable and consistent key performance indicators (KPIs) such as bandwidth and connections per second, which represents the real performance of the network infrastructure or device being tested with minimal user intervention. DuSIM's dual-objective support allows you to set multiple test objectives to determine if the underlying network infrastructure can achieve a specified throughput while maintaining a set number of simulated users. DuSIM can also gradually ramp-up the traffic load to the desired target in configurable increments for rate-based objectives (throughput and connections per second).

In this example, a subscriber range generates four application traffic streams and will configure an *Objective Type* for each stream. The OTT traffic type (shown in the image) can choose either Simulated Users or Throughput as its objective.



UI overview

The Keysight Open RAN Simulators Cloud Edition web UI provides access to all of the tools, functions, and options that are needed to create, run, and manage tests; to view, analyze, and manage test results; to respond to system events; and to administer your Open RAN Simulators Cloud Edition instance.

The major elements of the DuSIM UI are:

- [Dashboard page below](#)
- [Title bar and tool bars below](#)
- [Test Overview page below](#)
- [Configuration properties pages on the facing page](#)
- [Statistics page on the facing page](#)

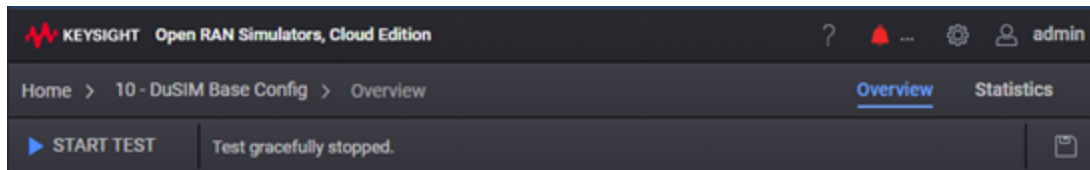
Dashboard page

After you successfully log in, the Dashboard page opens. From this page, you can create new tests, access other test sessions (each test session tile displays the test name and status), browse among and manage previously run tests, and browse among and access test results from previously run tests. You can navigate to the other Open RAN Simulators Cloud Edition pages to view and customize test setups, view real-time statistics, view and export test results, view events, logs, and other application and test-specific information.

You can return to the Dashboard at any time by clicking **Home** from the tool bar.

Title bar and tool bars

The Open RAN Simulators Cloud Edition UI presents a title bar at the top of the window and one or two tool bars underneath it. The presence of, and composition of, these bars dynamically changes based on your current actions.



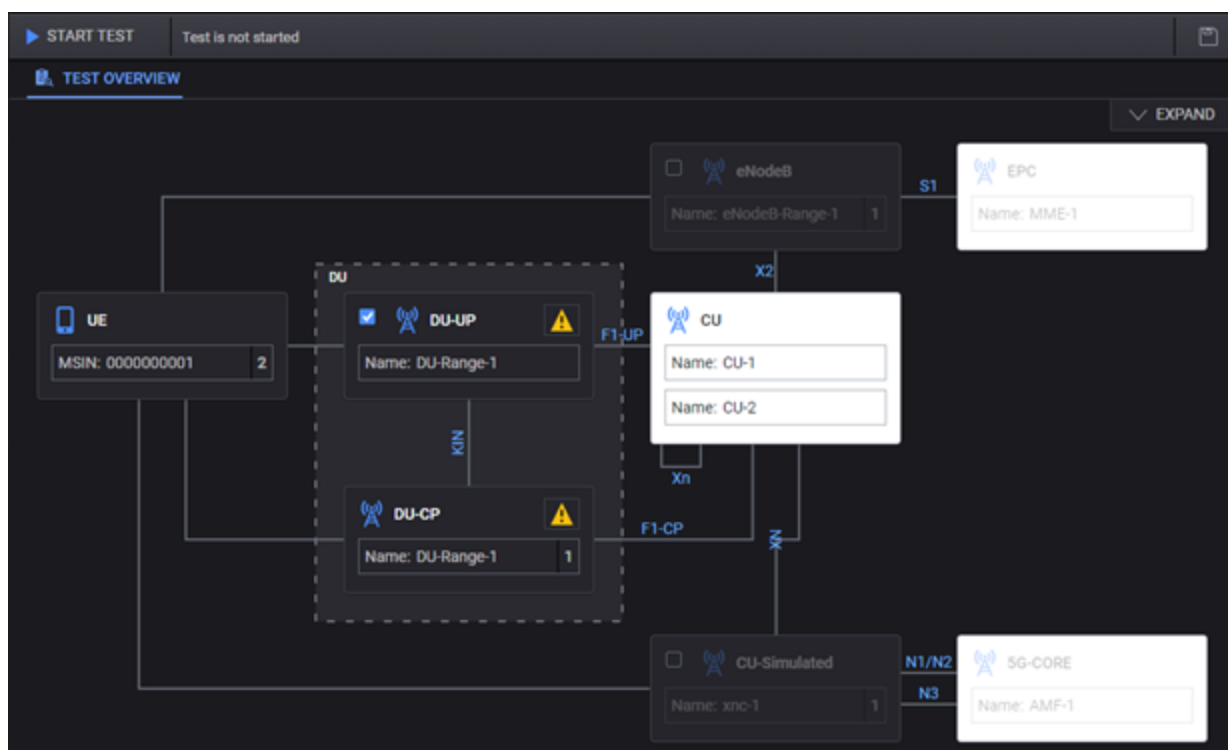
In addition to the information in this topic, refer to these topics for more information about the available tools and functions:

- [DuSIM title bar settings on page 222](#)
- [Save test sessions on page 205](#)

Test Overview page

When you open or create a test session based on any predefined, newly-created, or imported test configuration, DuSIM opens the **Test Overview** page (which you can collapse or expand as needed) on which you can view a summary of the test configuration and a visual representation of the test topology. The Overview includes a test progress bar, timeline and objectives summary data, a link to the Global Settings, and the test topology section.

The test topology is an interactive graphical representation of the test network. For example:



From the topology, you access all of the configurable elements for the current test. These include the DUT (your gNB-CU), the DU (DU-CP and DU-UP nodes), the user endpoints (UEs), eNodeB and EPC for NSA mode, CU-Simulated, and 5G-CORE.

In the example shown above, the dark blocks (UE, DU, eNodeB, and CU-Simulated) represent the simulated network components, while the white blocks (EPC, CU, and 5G-Core) represent the server-side elements.

Configuration properties pages

You use a number of properties pages as you configure a test. They are presented as a series of cascading panels that reveal successively detailed settings for the elements in your test configuration.

Statistics page

Real-time statistics are immediately available while a test is running and can be accessed for tests that were previously run. The statistics page will contain multiple panels that display graphical or textual test run statistics. You can select from among the various tabs to view specific categories of statistics, including F1 setup, F1 UE Context setup, F1 UE Context release, RRC procedures, NAS procedures, HTTP requests, HTTP traffic throughput, among others.

Open RAN Simulators Cloud Edition presents a default statistics dashboard, which is based on Grafana. You can change the dashboard to accommodate your own needs and select from many Key Performance Indicators (KPIs) that the agent exposes towards the middleware.

CHAPTER 2

Initial administrator login

This chapter describes the actions that are required the first time you log in to DuSIM as the application administrator, following deployment.

- [Required information below](#)
- [Initial login and password change below](#)
- [Activate licenses using License Manager on the next page](#)
- [Configure the License Server on the next page](#)
- [Create regular user accounts on page 16](#)

Required information

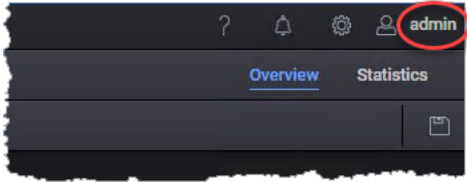
- The IP address that you set for the DuSIM web interface during deployment.
- The IP address of the license server.
The license server is shipped as a separate .ova file. After deploying the .ova file, you can access it using a web browser.
- Your DuSIM license activation codes (or entitlement codes).

Initial login and password change

DuSIM provides a default administrator account, and you will use that account on your initial login and for subsequent administrative tasks.

To log in as the administrator:

1. Enter the IP address of your deployed DuSIM instance in your browser's address field.
DuSIM opens the Keysight login page.
2. Enter the default administrator login credentials:
 - user ID: **admin**
 - password: **admin**
3. Click **Login**.
Because this is the initial login, DuSIM requires that you change the password for the admin account.
4. Review and accept the Keysight Software End User License Agreement.
5. Change the default **admin** user password:
 - a. Click your account name (*admin*) in the Keysight Open RAN Simulators, Cloud Edition 3.0 title bar.



Keysight Open RAN Simulators, Cloud Edition 3.0 opens the **Edit Account** page in a new browser tab.

- b. Click **Password** in the navigation pane.
- c. Enter the current password and your new password.
- d. Click **Save**.

Next steps:

- Activate licenses
- Configure your license server
- Create user accounts

Activate licenses using License Manager

Once you have completed the initial admin login, you need to activate the licenses for this DuSIM deployment.

To activate your licenses:

1. Select **Administration** from the setup menu (⚙️).
2. Select **License Manager** from the **Administration** menu. DuSIM opens the **License Manager** page.
3. To activate your licenses:
 - a. Select **Activate licenses**.
DuSIM opens the **Activate Licenses** dialog.
 - b. Enter your license data in the dialog box.
You can use either activation codes or entitlement codes (one or more).
 - c. Select **Load Data**, indicate the number of licenses you want to activate, then click **Activate**.
Your new licenses—which should now be listed in the **License Manager** page—are now available for running tests.

Configure the License Server

If you are using an external License server, then you need to select and configure your license provider:

1. Select **Applications Settings** from the setup menu (⚙️).
DuSIM opens the **Application Settings** dialog.
2. Select your **License Provider** from the drop-down list.
3. Enter the **License Server IP** address (see [Required information on the previous page](#), above).
4. Click **Update**.

Create regular user accounts

Before you and other members of your organization start building and running tests, it is recommended that you—logged in as the administrator—create a *regular user account* for each individual (including yourself). A *regular user* can create, manage, and run tests, but cannot perform access control functions (such as creating and managing user accounts). Further, it is recommended that you use the admin account only for administrative activities.

Refer to [Manage DuSIM users on page 219](#) for detailed information about user account management.

CHAPTER 3

User login and logout

Once the DuSIM application administrator has created user accounts for the individuals who will use DuSIM, those users can access the system and start to use its services.

Log in as a regular user

The user accounts that the DuSIM application administrator creates are known as regular user accounts. A *regular user* can create, manage, and run tests, but cannot perform access control functions (such as creating and managing user accounts).

1. Enter the DuSIM IP address in your browser's URL address field.
2. Press **Enter** to access the Keysight **Login** window.
3. Enter your Keysight Open RAN Simulators, Cloud Edition 3.0 username and password, then click **Login**.
4. If you are logging in for the first time, you may be required to change your password:
 - a. Enter your **New Password**.
 - b. Enter the password again in the **Confirm Password** field.
 - c. Click **Submit**.

Upon successful login, DuSIM opens the dashboard.

Log out

To log out of DuSIM, select **Log Out** from the Settings menu (⚙️).

*CHAPTER 4***Build and run a test**

This chapter describes the sequence of actions needed to build and run a new DuSIM test.

Chapter contents:

Step 1: Create a new test config	19
Step 2: Configure Global Settings	21
Step 3: Establish connectivity with your DUT	22
Step 4: Configure DU-CP test nodes	23
Step 5: Configure DU-UP test nodes	25
Step 6: Assign agents to the CU test nodes	26
Step 7: Configure eNodeB node	29
Step 8: Configure CU-Simulated node	31
Step 9: Configure mobile device definitions	33
Step 10: Create Scenario Groups	34
Step 10.1: Add and manage Scenario Groups	35
Step 10.2: Configure mobility	36
Step 10.3: Create Test Suites	38
Step 10.4: Defining parallel procedures	40
Step 11: Configure UEs	42
Step 12: Start the test	43
Step 13: View real-time test results	44

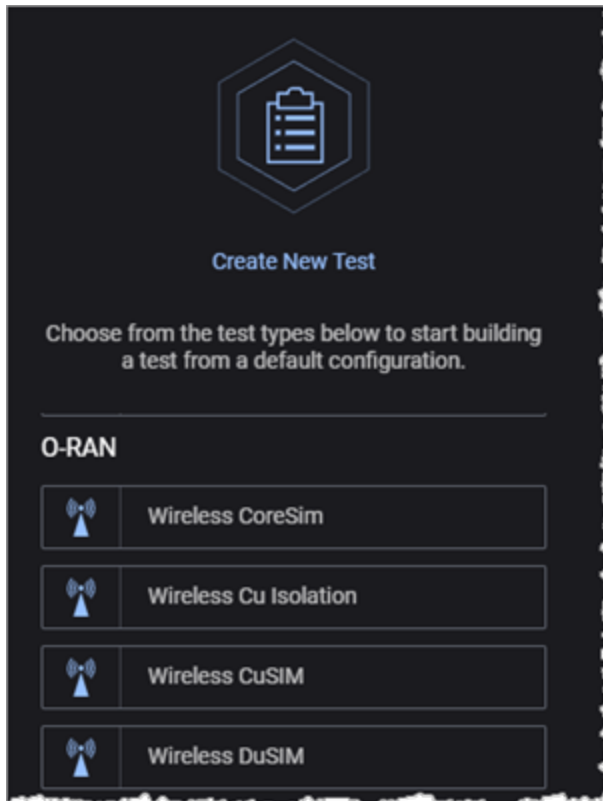
Step 1: Create a new test config

The first step in building a new test is to create a new config:

- [Create a config based on a template below](#)
- [Create a new config based on an existing config on the facing page](#)

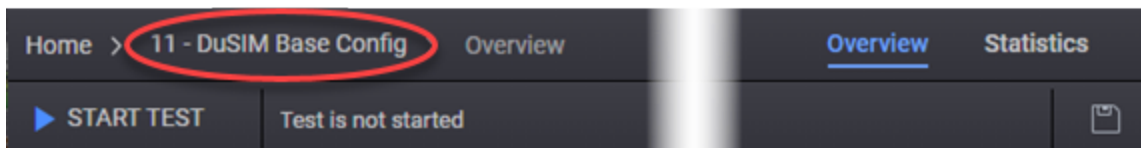
Create a config based on a template

1. Log in to DuSIM.
2. In the Dashboard page, select the **Wireless DuSIM** template from the **Create New Test** panel. For example:



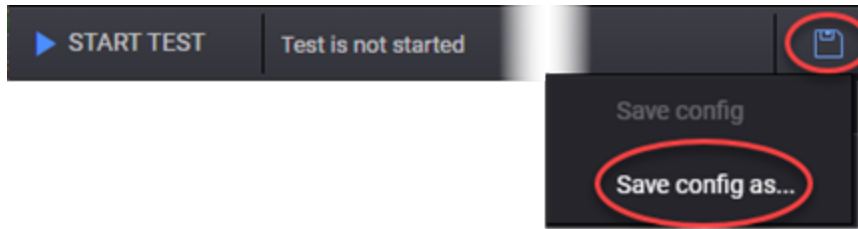
DuSIM opens the **Test Overview** page, which includes the graphical representation of the test topology. By default, SA topology is activated. You need to select NSA or CU-Simulated node for another network topology.

DuSIM assigns a session number and temporary name to the test, and displays that information in the title bar. For example:



3. Assign a name to your new test config:

- a. Select **Save config as...** from the disk icon (on the right side of the toolbar).



DuSIM opens the **Save config as** dialog.

- b. Enter a name for the config, then click **Save As**.

The new test config is immediately available.

NOTE

The terms *test config* and *test session* are not entirely synonymous. A "config" refers to a configuration definition file (JSON format), whereas a "session" is an instance of that file that is loaded in memory and is capable of being run. Refer to [Manage and use test sessions on page 204](#) for detailed information about managing config files and sessions.

Create a new config based on an existing config

Rather than creating a new config based on one of the DuSIM templates, you can create a config based on an existing test config. The only difference is that (in step 2 in the procedure shown above) you will select a test config from the **Browse Configs** panel, and that will be the source for your new config.

TIP

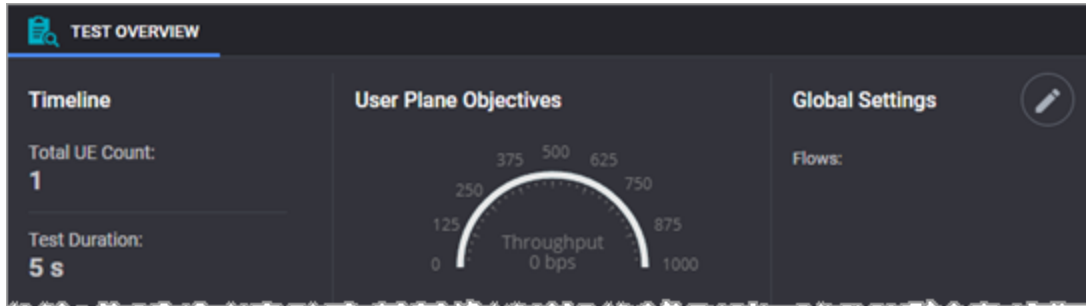
When planning the tests that you intend to run, you may want to create one or more "starter" configs of your own, rather than starting with a Keysight Open RAN Simulators, Cloud Edition 3.0 template. In effect, you can create private templates that are pre-populated with configuration values that you will typically use in your testing.

Step 2: Configure Global Settings

Global Settings provide access to configuration properties that are applicable at the test level (versus the node or UE level).

To configure the Global Settings:

1. Navigate to the **Test Overview** window.



2. Click **Expand** if the Test Overview section is collapsed.
3. Click the **Edit** button on the Global Settings section to open the **Global Settings** panel.

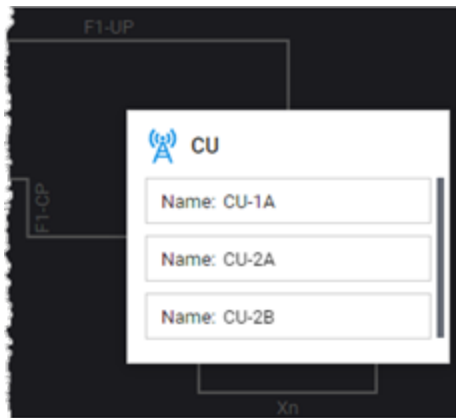


4. Configure the settings that you will need in your test.
Many of these settings are important for the proper execution of your tests and for establishing the parameters that control logging, captures, and statistics collection.

Refer to [Global Settings on page 46](#) for a description of all of the settings.

Step 3: Establish connectivity with your DUT

The DuSIM test topology includes a representation of your device under test (DUT).



The DUT will comprise one or more CU units that you are testing. For each CU unit, you need to configure IP values that enable communication with the DuSIM application.

In this step, you will:

1. Configure properties for the default CU node (CU-1) that is already present in the DuSIM test topology.
2. Optionally, add additional CU nodes to the topology, and configure each one.

For each CU node, you will specify the following configuration values:

- a name for the CU node (DuSIM provides a default name, which you can change),
- the gNB-CU identifier (CU-ID)
- the gNB-CU identifier length (CU-ID Length)
- the basic IP values for F1-C interface: address, prefix, and gateway. For NSA mode X2-C interface and Xn-C interface when connected to another simulated CU.

For detailed information, refer to [CU configuration settings on page 67](#).

Step 4: Configure DU-CP test nodes

The DuSIM test topology includes a representation of the simulated DU nodes in your test configuration. Each DU node is structured as two units: DU-CP and DU-UP.

To configure and manage DU-CP nodes for your test:

1. Select **DU-CP** from the topology window.
DuSIM opens the DU-CP **RANGES** panel. A new test will have one DU-CP range; you can add additional ranges.
2. Click the name of a range (such as DU-1) to access the configuration settings. For example:

The screenshot shows the 'DU-CP-Range' configuration window. On the left, the 'RANGES' panel lists two ranges: 'DU-Range-1' and 'DU-Range-2', each with a checked checkbox and a right-pointing arrow. On the right, the 'RANGE' configuration panel is shown for a selected range. It includes a dropdown for 'Associated CU' (CU-1), text input fields for 'DU ID' (1) and 'DU ID Length' (22), and a 'Range Count' field (1). At the bottom, there are two expandable sections under 'Range Settings': 'Cells' and 'F1-CP Interface Settings'.

3. Configure each of the settings, which are described in [DU-CP configuration settings on page 73](#).
4. To add and configure additional DU-CP ranges:
 - a. Return to the DU-CP **RANGES** panel.
 - b. Click the **Add Range** button.

NOTE

DuSIM automatically creates one DU-UP range for each DU-CP range that you configure in the test.

- c. Configure the settings for the new range.
5. To select or deselect a range for the test:

- a. Return to the DU-CP **RANGES** panel.
 - b. Click the **Select** check box to toggle the range between *Selected* and *Deselected*, as required.
6. To delete a DU-CP range:
- a. In the DU-CP **RANGES** panel, click the range to open its properties panel.
 - b. Click the **Delete Range** button. DuSIM deletes the range from your test config.

NOTE

If you delete a DU-CP range, DuSIM automatically deletes the corresponding DU-UP range.

Step 5: Configure DU-UP test nodes

The DuSIM test topology includes a representation of the simulated DU nodes in your test configuration. Each DU node is structured as two units: DU-CP and DU-UP.

About DU-UP ranges

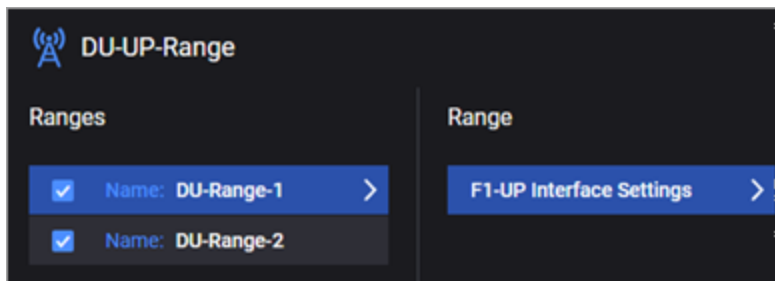
DuSIM manages DU-UP ranges as follows:

- DuSIM automatically creates one DU-UP range for each DU-CP range that you configure in the test.
- If you delete a DU-CP range, DuSIM automatically deletes the corresponding DU-UP range.
- Although you cannot directly delete a DU-UP range, you can deselect a range for the test session. When you deselect a DU-UP range, DuSIM does not deselect the corresponding DU-CP range.

How to configure DU-UP nodes

To configure and manage **DU-UP** nodes for your test:

1. Select **DU-UP** from the topology window.
DuSIM opens the DU-UP **RANGES** panel.
2. Click the name of a range (such as DU-1) to access the configuration settings. For example:



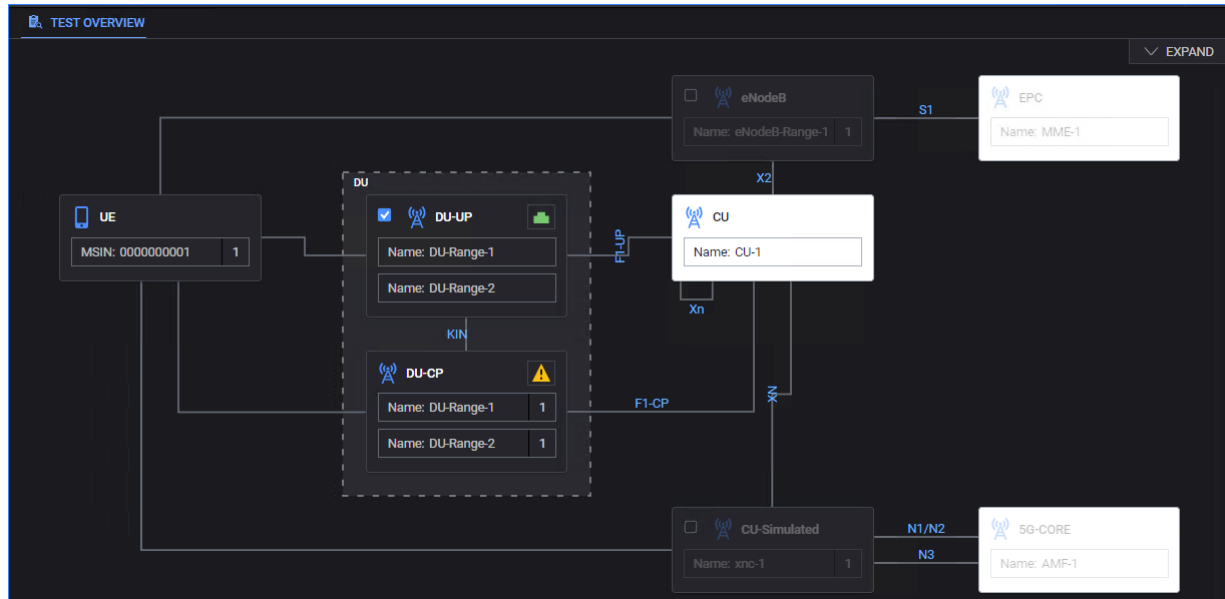
3. Configure each of the settings, which are described in [DU-UP Range panel on page 90](#).
4. To select or deselect a range for the rest:
 - a. Return to the DU-UP **RANGES** panel.
 - b. Click the **Select** check box to toggle the range between *Selected* and *Deselected*, as required.

Step 6: Assign agents to the CU test nodes



You cannot run a DuSIM test until you have assigned agents to all of the test nodes. To assign an agent to a node:

1. In the topology window, select the traffic agent icon on the top right corner of the node.

For example:



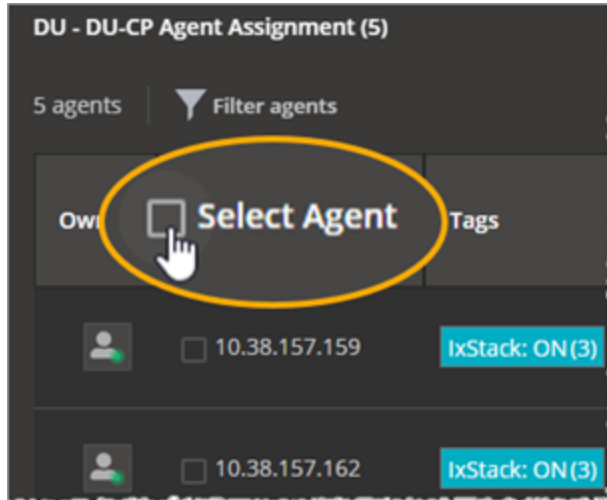
The icon that represents the agent can be any of the following:

-  — No agents are assigned to the node.
-  — One or more agents are assigned.

DuSIM opens the **Agents Assignment** window, which presents a list of agents. If the list has no filters set, then all agents are listed.

2. Assign specific agents or all available agents to the node:
 - To assign specific agents (one or more) to the node, select the check-box next to the agent's IP address.

To assign all available agents to the node, select the **Select Agent** check-box (located in the table header).



Note that you can display the agent ID by hovering over the IP address.

3. Select the F1 and KIN **Connections**, if required.
4. Click **Update**.

Agent Assignments window

The following table describes the content of each column displayed on the **Agents Assignment** window.

Column	Description
Owner	<p>Hover over the Owner icon to see the current agent ownership and status, which will be one of the following:</p> <ul style="list-style-type: none"> The agent is owned by the user whose email address is listed. In this case, the agent is not available for assignment. The agent is offline. In this case, the agent is not available for assignment. The agent is available for assignment.
Select Agent	<p>Use the check box next to the IP address to select that agent for assignment. You can also select all available agents by selecting the Select Agent check box (in the table header).</p>
Tags	<p>This column displays the tags associated with each agent. Each tag indicates the number of agents to which it is associated.</p> <p>Refer to About traffic agents on page 59 for more information about tags.</p>
Connections	<p>The table displays the available interface and the MAC address for each wireless connection. The interface can be selected from the drop-down list.</p> <div style="display: flex; align-items: center;"> <div style="background-color: #cccccc; padding: 5px; margin-right: 10px;">NOTE</div> <p>For the DuSIM nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.</p> </div>

NOTE

From the **Agents Assignment** window you can select other nodes from the list and configure the agents for those nodes also. In this way, you can configure agents for all your test nodes at the same time.

See also, [Assign and manage agents on page 58](#).

Step 7: Configure eNodeB node

If you are configuring an NSA mode topology, you must select eNodeB node. After you select eNodeB, both eNodeB and EPC (4G Core) node will be activated in the Topology diagram.



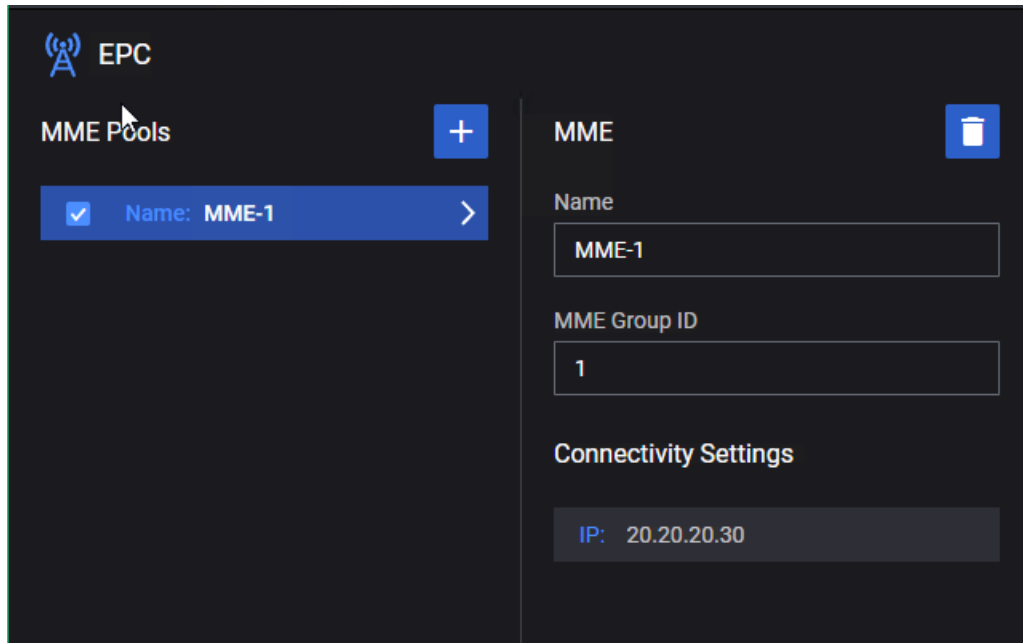
The interface is titled 'eNodeB' with a radio tower icon. It is divided into two main sections: 'RANGES' and 'RANGE'.

RANGES section: Contains a list with one item: 'Name: eNodeB-Range-1' with a checkmark and a right arrow. A blue '+' button is at the top right.

RANGE section: Contains configuration fields for the selected range. A blue trash icon is at the top right.

Field	Value
Name	eNodeB-Range-1
eNodeB ID	1
Range Count	1
Associated MME	MME-1

- eNodeB does not need any Agent specifically to assign. It runs on previously assigned agents for DU-CP node.
- EPC needs to be configured when eNodeB is enabled. See [EPC configuration settings](#).



Step 8: Configure CU-Simulated node

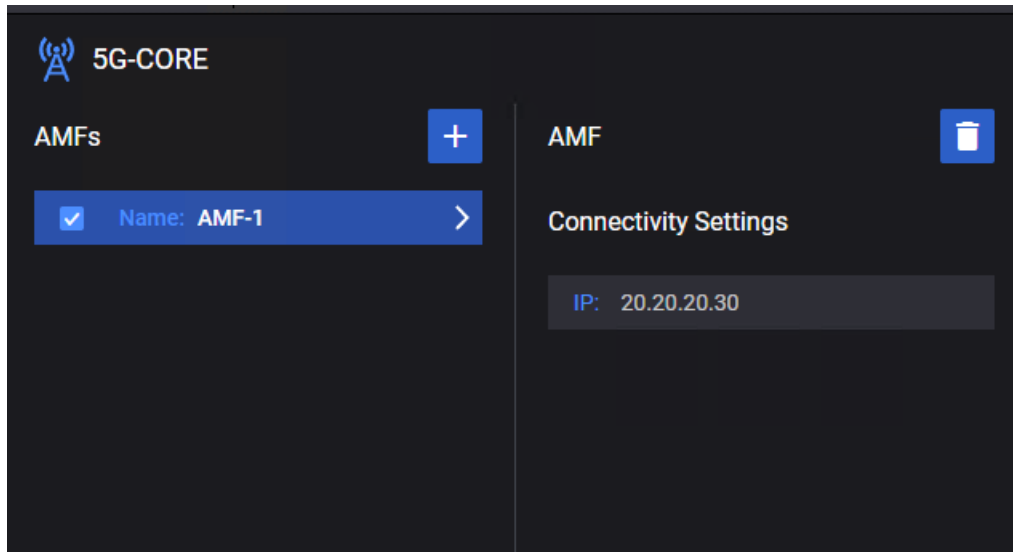
CU-Simulated node is selected when Xn interface towards DUT CU is simulated in SA mode. Once CU-Simulated node is selected both CU-Simulated and 5G-CORE node will be activated in the Topology diagram.



The configuration screen for the 'CU-Simulated' node is divided into two main sections: 'RANGES' and 'RANGE'.

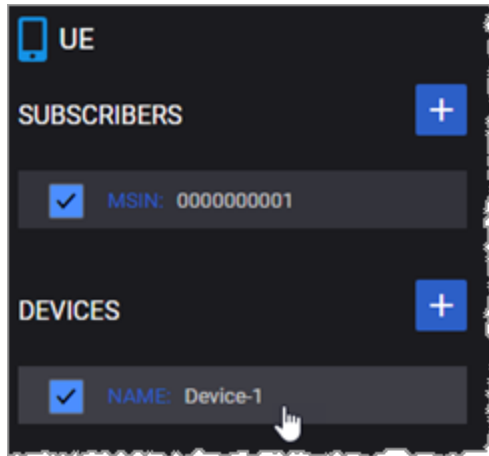
- RANGES:** Contains a list with one entry: 'Name: xnc-1'. There is a plus icon to add more ranges.
- RANGE:** Contains a list of settings: 'Node Settings', 'Cell Settings', 'Subscriber Settings', 'N2 Interface Settings', 'N3 Interface Settings', 'Xn-C Interface Settings', and 'Xn-U Interface Settings'. There is a trash icon to delete the range.

- CU-Simulated node does not need to assign any Agent specifically. It runs on same agents previously assigned for DU-CP node.
- 5G-CORE node needs to be configured when CU-Simulated node is enabled. See [5G-CORE configuration settings](#).



Step 9: Configure mobile device definitions

In a DuSIM test, each range of simulated subscribers will select a **DEVICE** range; each such range specifies the properties of a mobile device type that is used by all of the subscribers in the **SUBSCRIBERS** range. You can create as many device ranges as needed in a test, and each device range can be associated with multiple subscriber ranges.



To configure one or more ranges of mobile device definitions for a test:

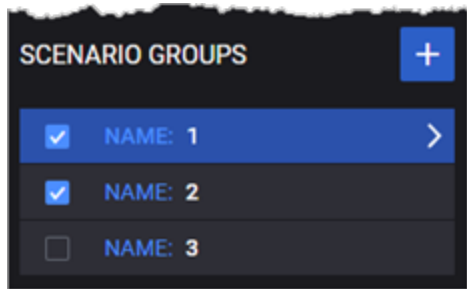
1. Select **UE** from the DuSIM topology window.
DuSIM opens the top-level (leftmost) UE properties window.
2. From the UE panel, click a **DEVICES** range (such as Device-1) to open its properties panel.
3. Configure the device settings, as described in [UE Device settings on page 149](#).
4. To add and configure additional device ranges:
 - a. Return to the UE **DEVICES** panel.
 - b. Click the **Add Range** button.
 - c. Configure the settings for the new range.
5. To select or deselect a range for the rest:
 - a. Return to the UE **DEVICES** panel.
 - b. Click the **Select** check box to toggle the range between *Selected* and *Deselected*, as required.
6. To delete a device range:
 - a. In the UE **RANGES** panel, click the range to open its properties panel.
 - b. Click the **Delete Range** button. DuSIM deletes the range from your test config.

Step 10: Create Scenario Groups



You access SCENARIO GROUPS from the top-level (leftmost) UE property panel. From this panel, you add scenario groups and access their properties panels.

Refer to [Scenario Group settings on page 170](#) for detailed descriptions of the configuration settings.



SCENARIO GROUPS define the detailed control plane traffic that enables the subscribers to access the network and successfully transmit user plane traffic.

The tasks involved with creating, configuring, and managing SCENARIO GROUPS are described in the following subtopics:

Step 10.1: Add and manage Scenario Groups	35
Step 10.2: Configure mobility	36
Step 10.3: Create Test Suites	38
Step 10.4: Defining parallel procedures	40

Step 10.1: Add and manage Scenario Groups



You access SCENARIO GROUPS from the top-level (leftmost) UE property panel. From this panel, you add and manage the Scenario Groups that you need for your test.

This topic describes the following Test Suite actions:

- [Select a Scenario Group for editing below](#)
- [Add a new Scenario Group to your test below](#)
- [Delete a Scenario Group below](#)

Select a Scenario Group for editing

To select a Scenario Group for editing or viewing:

1. Click **UE** in the topology window to open the UE properties panel.
2. From the top-level (leftmost) **UE** property panel, click a **SCENARIO GROUPS** entry (DuSIM assigns each group a number). DuSIM opens its properties panels.

Add a new Scenario Group to your test

1. Click **UE** in the topology window to open the UE properties panel.
2. Click the **Add Scenario Group** button. DuSIM adds the new group and assigns it a number.

Delete a Scenario Group

To delete a Scenario Group from your test:

1. Click **UE** in the topology window to open the UE properties panel.
2. Select the Scenario Group that you will delete.
3. Click the **Delete Scenario Group** button. DuSIM immediately removes it from the test configuration.

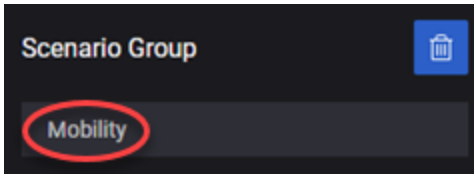
Step 10.2: Configure mobility

Each Scenario Group can configure UE mobility actions.

1. Click **UE** in the topology window to open the UE properties panel.

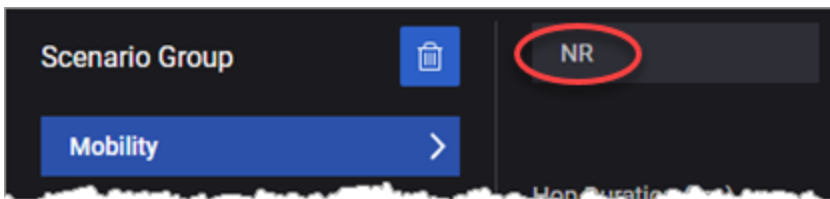


2. Select the **Scenario group** for which you are configuring mobility.
DuSIM opens its properties panel, which is where you access the Mobility settings.
3. Select **Mobility** from the Scenario group properties panel.



DuSIM opens a new panel to display the **Mobility** settings (which are described in [Mobility settings on page 172](#)).

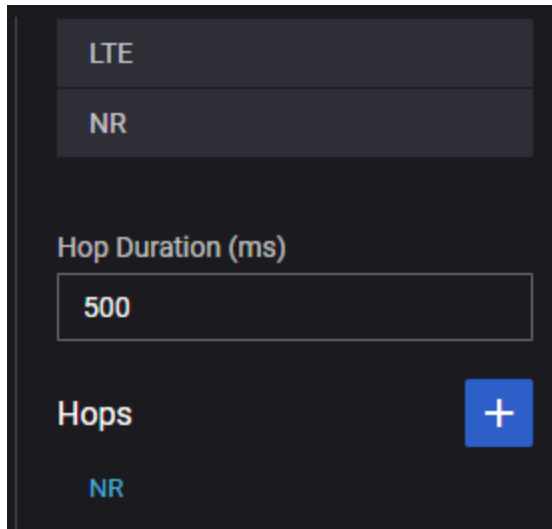
The settings that appear vary depending upon whether your test is configured for SA or NSA testing. For example, if the test is configured for SA, you will have access to the 5G mobility test settings:



4. Configure the SA and/or NSA nodes and strategy:
 - a. If your test is configured for SA testing:
 - i. Click **NR**.
DuSIM opens a new panel.
 - ii. In the *DU* field, select the DU range for the mobility event.
 - iii. In the *Strategy* field, select the mobility type: Intra DU, Inter DU, or Inter CU.
 - b. If your test is configured for NSA testing:
 - i. Click **LTE**.
DuSIM opens a new panel.
 - ii. In the *eNodeB* field, select the eNodeB range for the mobility event.
 - iii. In the *Strategy* field, select the mobility type: Intra eNB or Inter eNB.

5. Configure the mobility event hops:

- a. Click the **Add Hop** button to add a hop definition. DuSIM adds an **NR** link to the panel.



- b. Click the **NR** link. DuSIM adds a **Hop** panel.
- c. In the **Hop** panel, select the *Step Type*, which can be NR or LTE.
If you change the *Step Type*, DuSIM will reflect that change in the link (which is located on the panel to the left of the Hop panel).
- d. Enter the *Number of Hops*.
For example, if the DU-CP has five cells and you specify a *Number of Hops* value of 4, the UE can move from cell 1 to cell 2 (first hop), then to cell 3 (second hop), then to cell 4 (third hop), then to cell 5 (fourth hop): each move is a hop.
- e. Repeat these steps to add additional Hops definitions.

6. Specify the Hop Duration for the mobility events.

This is the amount of time (in ms) that will elapse between hops.

Notice that you do not select individual DUs for the attach and handover procedures. Depending on the mobility *Strategy* that you select, DuSIM chooses the DUs with which the UEs will perform the initial attach and handovers. With DuSIM automatically making these choices, it is not difficult to scale the mobility simulation for thousands of UEs and thousands of DUs.

Step 10.3: Create Test Suites

DuSIM Test Suites are defined and managed as part of the UE SCENARIO GROUPS settings.

This topic describes the following Test Suite actions:

- [Accessing the Test Suite settings below](#)
- [Add a Test Suite below](#)
- [Delete a Test Suite below](#)
- [Build a Test Procedures call flow on the next page](#)
- [Create parallel procedures on page 40](#)

Accessing the Test Suite settings

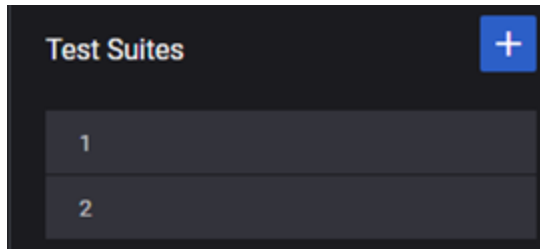
1. Click **UE** in the topology window to open the UE properties panel.



2. From the top-level (leftmost) UE property panel, click a Scenario Group (DuSIM assigns each group a number).

DuSIM opens its properties panel, which is where you create and access Test Suites settings.

Add a Test Suite



Each Scenario Group will have one or more Test Suites, each of which defines a procedural call flow for the test.

To add a Test Suite to a selected Scenario Group:

1. Select the Scenario Group to which you will add the new Test Suite.
2. Click the **Add Test Suite** button. DuSIM adds a new Test Suite and assigns it a number.
3. Click the new Test Suite to open its first properties panel.

Refer to [Test Suite settings on page 175](#) for a description of the Test Suite configuration settings.

Delete a Test Suite

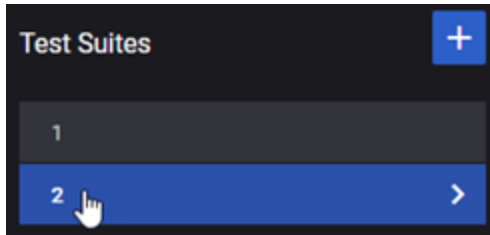
To delete a Test Suite from a selected Scenario Group:

1. Select the Scenario Group from which you will delete the Test Suite.
2. Click the **Test Suite** number to select it. DuSIM will open its properties panel.
3. Click the **Delete Test Suite** button to delete it from the Scenario Group.

Build a Test Procedures call flow

Each test suite needs a procedural call flow: a set of procedures that DuSIM will call, in order, during test execution. To build the call flow for a test suite:

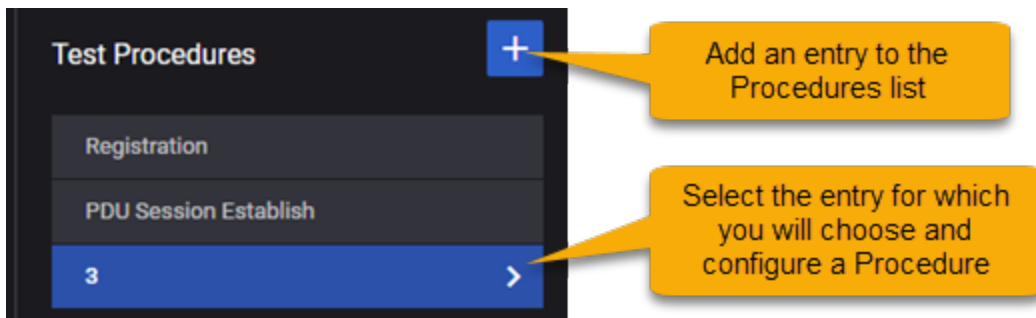
1. Select the desired suite from the list of Test Suites.



DuSIM opens the **Test Suite** properties panel.

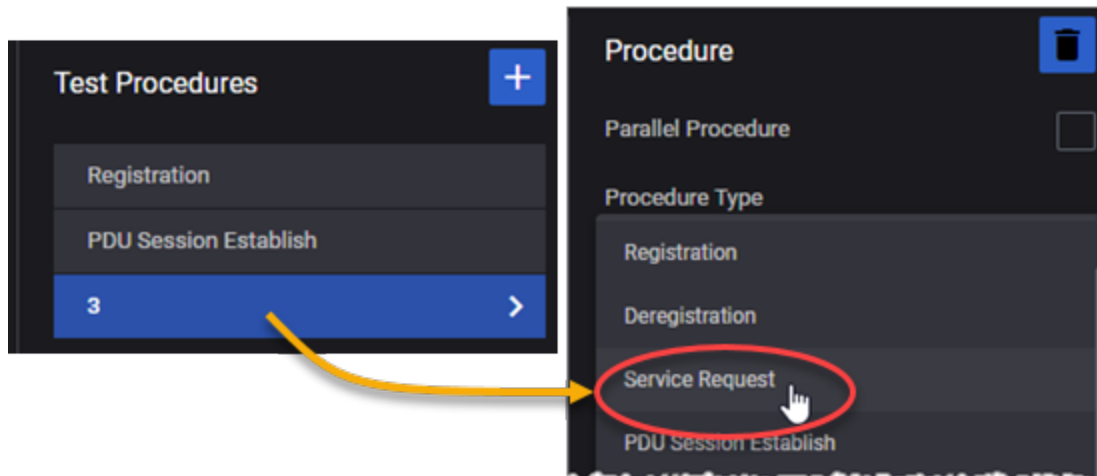
2. Configure the registration attempts and repetitions for the test suite:
 - Enter a *Call Attempt/s* value: the number of registration procedures to attempt per second.
 - Specify the number of times that the procedural call flow will repeat. You can set it for either a specific number of repetitions or a continuous loop.

Refer to [Test Suite settings on page 175](#) for detailed descriptions of these properties.
3. Select and configure the specific procedures that this test suite will execute:



- a. Click the **Add Test Procedure** button. DuSIM adds an entry to the list, and displays its sequence number.
- b. Select the newly-added procedure.
DuSIM opens the **Procedure** panel.

- c. Select a procedure from the *Procedure Type* drop-down list. For example:



DuSIM updates the call flow and displays the configuration settings for that specific procedure.

- d. Configure the settings for the newly-added procedure.
Refer to [Test procedures for SA on page 176](#), [Test procedures for NSA tests on page 184](#), and [Test procedures for SA and NSA on page 198](#) for a description of the Procedure configuration settings..
- e. Please contact Technical Support for assistance with the *Parallel Procedure* option.
- f. Repeat these steps to add additional entries to the call flow.

NOTE

The Registration/Attach procedure is required in every call flow. Deregistration/Detach is recommended, and all others are optional.

4. To delete a procedure from the call flow, select it and then click the **Delete Test Procedure** button.

Create parallel procedures

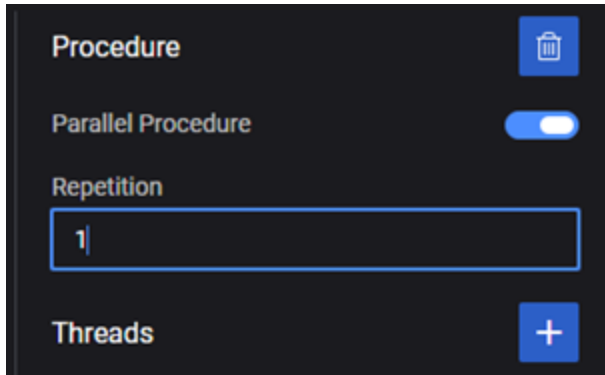
You can also configure any of the test procedures as multi-threaded parallel procedures. For instructions, refer to [Defining parallel procedures below](#).

Step 10.4: Defining parallel procedures

Each DuSIM Scenario Group that you define requires a procedural call flow: the procedures that will be sequentially initiated when the test starts. Each of the procedures in the call flow can optionally specify parallel procedures. When you enable the parallel procedure option for a procedure in your call flow, you then configure multiple threads for that specific procedure.

To configure a parallel procedure:

1. In the **Test Suite** panel, select the procedure for which you will create the parallel procedure. Enable the *Parallel Procedure* option and set the *Repetition* value.



Repetition specifies the number of times that the parallel procedure will execute for each iteration of the main procedure.

Notice that DuSIM changes the panel to show a new **Threads** option.

Click the **Add Thread** button.

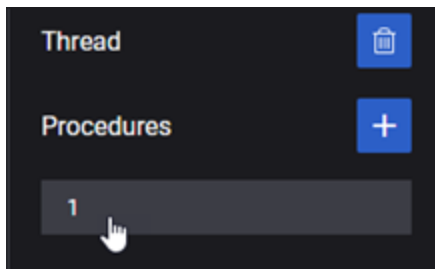


DuSIM adds a new numbered entry for which you will configure a thread.

4. Click the new Threads entry (which is identified as a number).

DuSIM opens a new *Thread* panel on the right. This new panel has options to delete the thread or to add a procedure to the thread.

In the new Thread panel, click the **Add Procedure** button.



DuSIM adds a new numbered entry for which you will configure a thread. As you add entries, they are initially assigned numbers. When you select a procedure for the entry, the number will be replaced by the procedure name.

6. Click the new entry (shown as 1 in the example above).

DuSIM opens a new *Procedure* panel on the right. This new panel has options to delete the procedure or to select the parallel procedure for the thread.

7. Select the procedure, then configure its values.

Refer to [Test procedures for SA on page 176](#), [Test procedures for NSA tests on page 184](#), and [Test procedures for SA and NSA on page 198](#) for a description of the Procedure configuration settings.

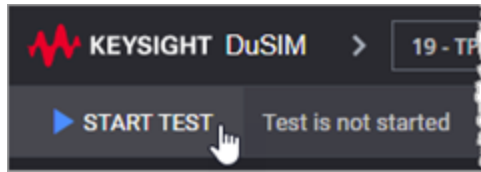
8. Repeat these steps to add additional threads to the selected procedure.

Step 11: Configure UEs

To configure one or more ranges of mobile UE definitions for a test:

1. Select **UE** from the DuSIM topology window.
DuSIM opens the top-level (leftmost) UE properties window.
2. From the UE panel, click a **UE** range to open its properties panel. (Each range is identified by the MSIN assigned to the first UE in the range.)
DuSIM opens the **RANGE** for the selected MSIN.
3. Configure the UE settings. The configuration tasks for each range include:
 - a. Specify the number of UEs to create for the range (the *Range Count* setting).
 - b. Select a range for each of the following: *Associated Device* and *Scenario Group*.
 - c. Configure the detailed settings, which include the range's Identity settings, SIM settings, ESM settings, EMM settings, DNN settings, Network Slicing settings, and NR provisioning.
Refer to [UE configuration settings on page 133](#) for detailed descriptions.
 - d. Configure the Protocol Configuration Options in the ESM settings:
 - i. From the Subscriber **ESM** settings panel, select the **Configure** button in the *Protocol Configuration Options* field.
 - ii. Please contact Technical Support for assistance with this option.
 - e. Configure **Objectives** for the range:
 - i. In the **RANGE** panel, click **User Plane** (in the **Objectives** section).
DuSIM opens the **User Plane** panel.
 - ii. Add each **Application Traffic** type that you need for the subscriber range.
The application traffic types include Stateless UDP, Data, Voice, Video OTT, and DNS Client.
Refer to [UE Test Objective settings on page 151](#) for a description of the properties that you can configure for each of the traffic types.
4. To add and configure additional UE ranges:
 - a. Return to the UE panel.
 - b. Click the **Add Range** button.
 - c. Configure the settings for the new range.
5. To select or deselect a range for the test:
 - a. Return to the **UE** panel.
 - b. Click the **Select** check box to toggle the range between *Selected* and *Deselected*, as required.
6. To delete a UE range:
 - a. Select the range from the **UE** panel.
DuSIM opens that UE **RANGE** panel.
 - b. Click the **Delete Range** button. DuSIM deletes the range from your test config.

Step 12: Start the test



Once you have configured all the properties needed for your test, click the **START TEST** button.

Once you start a test, the DuSIM tool bar displays the test status throughout its execution progress. In addition, each test session tile (located on the DuSIM Dashboard) displays that test's name and current status. The test status will be one of the following:

- **Test is not started:** The test session is created, the test configuration is loaded, but the test has not yet been started.
- **Test is initializing:** After clicking the **START TEST** button on the test progress bar, the initializing state is displayed on the progress bar and the test session tile. During this phase the hardware resources are allocated and the test is prepared for starting.
- **Test is configuring:** During this stage, the configuration is applied to the test.
- **Test is running:** During this stage, the nodes are connected, test iterations start one-by-one based on the configured parameters, traffic flows are connected, and traffic generation begins.
- **Test is stopping:** During this stage, traffic stops, traffic flows disconnect, logs are collected, ports are released, and the hardware disconnects.
- **Test is stopped:** The test is no longer running.

DuSIM will display a message in the tool bar if it cannot successfully initialize the test.

Once the test initialization and configuration phases have been successfully completed, DuSIM will:

- Start generating traffic (user plane and control plane).
- Display the **STOP TEST** button in the tool bar.
- Open the **STATISTICS** page.

The estimated total time it takes the test to complete and the current run time are also displayed on the progress bar.

If for any reason you want to stop the test before it completes, select the **STOP TEST** button on the progress bar. DuSIM will perform a graceful shutdown of the test, assuming that you have enabled the **Graceful Shutdown Enabled** option in the **Global Settings** window (one of the **Session Settings**).

Step 13: View real-time test results

When you successfully start a test, DuSIM immediately displays the **STATISTICS** page, where you can view real time statistics.

The specific groups of statistics that are collected depend upon several factors, including:

- The types of traffic that you have chosen in your **Objectives** settings.
- Whether or not you have selected **Enable User Plane Advanced Stats** in the **Global Settings** (one of the **Advanced Settings**).
- The procedural call flows that you have established in the **Test Suites** defined for the test.

Statistics page

The **Statistics** page has several panels, which can be dragged and dropped and rearranged on the dashboard. They can also duplicated or removed, and there are a wide variety of formatting options for each panel. Inspecting a panel allows you to view or download results as CSV, JSON, Query, or just as a list of Stats.

NOTE

Open RAN Simulators Cloud Edition presents a default statistics dashboard, which is based on Grafana. You can change the dashboard to accommodate your own needs and select from many Key Performance Indicators (KPIs) that the agent exposes towards the middleware.

Statistics groupings

The statistics are organized into groups, which include Overview, Application Traffic, and Agent Statistics

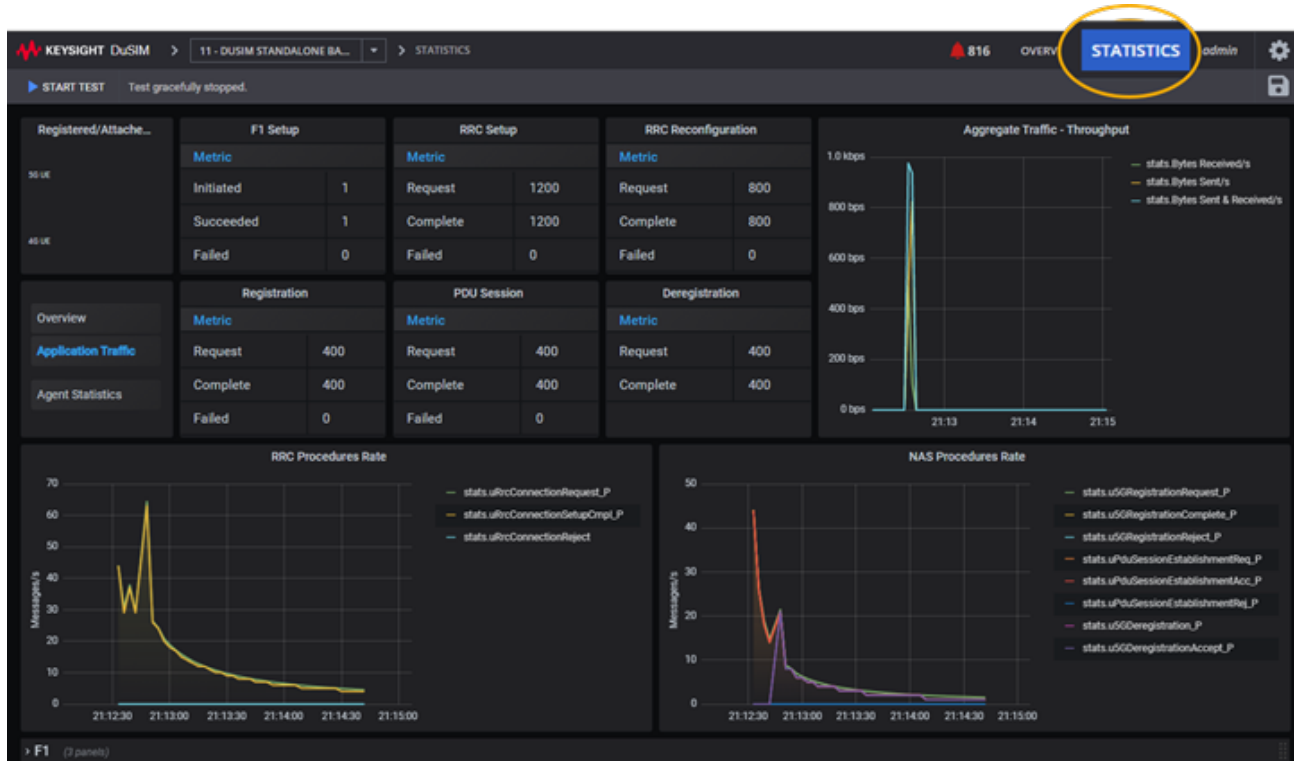
Overview statistics include:

- F1 Setup: number of procedures initiated, succeeded, and failed.
- RRC Setup: number of procedures initiated, succeeded, and failed.
- RRC Reconfiguration: number of procedures initiated, succeeded, and failed.
- Registration: number of procedures initiated, succeeded, and failed.
- PDU Session: number of procedures initiated, succeeded, and failed.
- Deregistration: number of procedures initiated, succeeded, and failed.
- Aggregate Traffic Throughput: number of bytes sent and received per second.
- RRC Procedure Rate: number of RRC connections requested, completed, and rejected per second.
- NAS Procedure Rate: number of NAS registrations and deregistrations requested, completed, and rejected per second; number of PDU session establishment requests made, accepted, and rejected.

Application Traffic statistics include:

- DU user plane Throughput Distribution: current and percentage BPS, per protocol.
- User Plane Throughput: DU user plane traffic, L2-3 Device Tx Traffic, L2-3 Device Rx Traffic (kbps).
- Application traffic detailed statistics, per protocol (TCP, GTPu, and so forth).

The **Agent statistics** display agent CPU and memory usage data.

Statistics page example

CHAPTER 5

Global Settings

The Global Settings are a list of parameters that have overall applicability to DuSIM tests and can be used to define resources or limits for nodes and UEs. It is recommended that you configure the Global Settings before proceeding with the node or the UE configurations of your test.

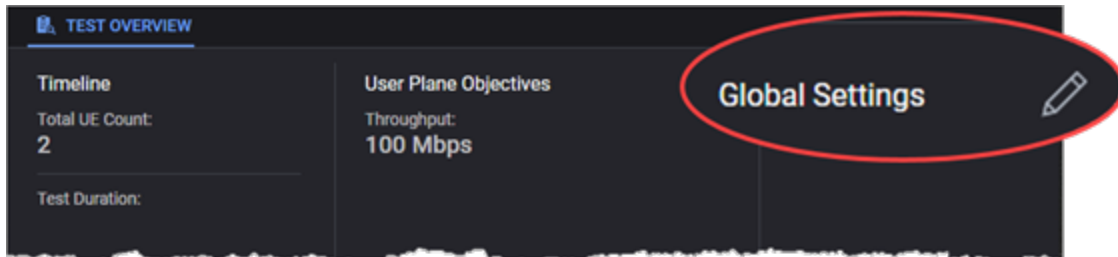
Chapter contents:

Access Global Settings	47
Technical Spec Version	48
DNS Settings	48
Advanced Settings	49
Impairment Settings	54
Session Settings	55
DNNs Settings	55
MMW Settings	56
TM Settings	57
CA Certificates Settings	57

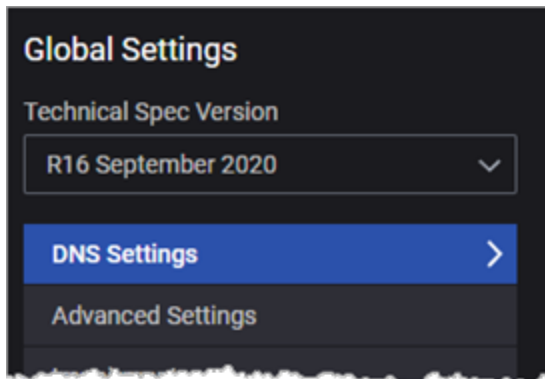
Access Global Settings

To access the **Global Settings** page, do the following:

1. Select the **Test Overview** tab.
2. Click **Expand** if the **Test Overview** section is collapsed.
3. Click the **Edit** button on the Global Settings section.

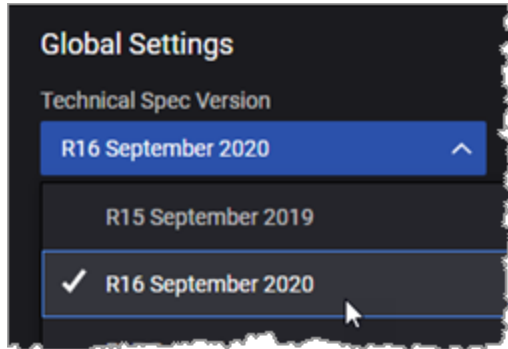


This opens the **Global Settings** panel.





Technical Spec Version

The DuSIM Global settings provide an option for selecting from among the available 3GPP Technical Specifications.



DNS Settings

The following table describes the settings required for the DNS Resolver configuration.

Setting	Description
Cache Timeout (ms)	The amount of time (in milliseconds) the local DNS stores the address information.
<i>DNS Name Servers:</i>	
	Click the Add DNS Name Server button to add a new DNS server to your test configuration. Set the IP address of the DNS server.
	Click the Delete button to remove the DNS server from your test configuration.

Advanced Settings

The following Global settings are available from the Advanced Settings panel:

- [Advanced Settings below](#)
- [Logging Settings on the facing page](#)
- [Traffic Settings on page 53](#)
- [KIN Interface Settings on page 53](#)

Advanced Settings

The Advanced Settings include the following:

Setting	Description
Overwrite Capture Size	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size	This option becomes available only when <i>Overwrite Capture Size</i> is enabled. It allows you to set the custom value of the capture size for IxStack.
Enable Capture Circular Buffer for IxStack	Select this option to enable circular buffer capture for IxStack.
Enable Capture On Loopback Interface	Select this option to enable packet capture on the loopback interface.
Enable Control Plane Advanced Stats	Select this option to enable control plane latency statistics.
Enable User Plane Advanced Stats	<p>Select an option from the drill-down list for the user plane advanced statistics:</p> <ul style="list-style-type: none"> • None - no advanced statistics enabled. • One Way Delay - the time spent by the packet on the network from the moment it is sent until it is received. • Delay Variation Jitter - the per polling interval average delay variation jitter value calculated for all packets.
Automated Polling Interval	This option is enabled by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval (sec)	<p>This option becomes available only when <i>Automated Polling Interval</i> option is disabled.</p> <p>It allows you to set a custom polling interval.</p>

Logging Settings

The Logging Settings are accessed from the Advanced Settings Panel. The following tables describe log level and log components settings:

Agent:

Setting	Description
Log level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful for debugging the application.
Log Tags	<p>Log Tags are used to collect specific information in the logs; they work with Debug and with Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.</p> <p>Select one or more tags from the drop-down list.</p>

GTPU:

Setting	Description
Log level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Critical - Designates messages indicating that a major error has occurred that impacts system stability. • Error - Designates messages indicating that an error has occurred that impacts application stability. • Warning - Designates messages indicating that an error has occurred that potentially impacts application stability. • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful for debugging the application.
Log Components	<p>These are different protocol pieces, or subcomponents, of the GPRS Tunnelling Protocol GTP overall functionality. This limits the amount of information that is collected, making it easier for you to extract the data that you need, as it does not log full packets that are received, but logs different events which helps in debugging on the selected component.</p> <p>Select one or more components from the drop-down list.</p>
Log Frame Components	<p>This option logs actual packets on the wire as the GPRS Tunnelling Protocol processes it, so here you can select which packet you want to log, like: Uplink packet, Downlink packet, ARP packet, etc.</p>

Setting	Description
	Select one or more components from the drop-down list.

Control Plane PDCP:

Setting	Description
Log level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Critical - Designates messages indicating that a major error has occurred that impacts system stability. • Error - Designates messages indicating that an error has occurred that impacts application stability. • Warning - Designates messages indicating that an error has occurred that potentially impacts application stability. • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates informational messages that highlight the progress of the application at coarse-grained level.
Log Components	<p>These are different protocol pieces , or subcomponents of the Packet Data Convergence Protocol overall functionality. This limits the amount of information that is collected, making it easier for you to extract the data that you need, as it does not log full packets that are received, but logs different events which helps in debugging on the selected component.</p> <p>Select one or more components from the drop-down list.</p>

User Plane PDCP:

Setting	Description
Log level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Critical - Designates messages indicating that a major error has occurred that impacts system stability. • Error - Designates messages indicating that an error has occurred that impacts application stability. • Warning - Designates messages indicating that an error has occurred that potentially impacts application stability. • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful for debugging the application.
Log Components	<p>These are different protocol pieces , or subcomponents of the Packet Data Convergence Protocol (PDCP) overall functionality. This limits the amount of information that is collected, making it easier for you to extract the data that you need, as it does not log full packets that are received, but logs different events</p>

Setting	Description
	<p>which helps in debugging on the selected component.</p> <p>Select one or more components from the drop-down list.</p>

F1APSM - F1 Application Protocol (F1AP) State Machine

Setting	Description
Log level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Critical - Designates messages indicating that a major error has occurred that impacts system stability. • Error - Designates messages indicating that an error has occurred that impacts application stability. • Warning - Designates messages indicating that an error has occurred that potentially impacts application stability. • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful for debugging the application.
Log Components	<p>Log Components are used to collect specific information in the logs. Rather than allowing the logs to collect information about everything, you can use Log Components to collect logging events related to the processing of the F1 Application Protocol. This limits the amount of information that is collected, making it easier for you to extract the data that you need.</p> <p>Select one or more components from the drop-down list.</p>

TM - Test Manager:

The Test Manager is a process that is responsible for the RRC and NAS protocol state machine and controls the full test.

Setting	Description
Log Level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • None - The application does not collect any log information related to the TM. • Error - Designates messages indicating that an error has occurred that impacts application stability. • Critical - Designates messages indicating that a major error has occurred that impacts system stability. • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful for debugging the application.

Setting	Description
Number of Secondary Processes	Specify the number of secondary processes. The TM works in primary-secondary process module , where primary processes distributes work on secondary processes. As we increase secondary processes, system performance can be increased at the cost of CPU cores that would be needed to scale the secondary processes.

Traffic Settings

The following table describes the settings on the Traffic Settings panel:

Setting	Description
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable Real-time Transport Protocol (RTP).
Cores	The number of cores reserved for RTP transmission.
Enable Jumbo Frame	Enable this option if your test traffic requires the use of jumbo frames (Ethernet frames with more than 1500 bytes of payload). When you enable this option, the you can configure any of the MTU parameters in the test to any valid jumbo frame size (up to 9,000 bytes).

KIN Interface Settings

The traffic agents of the DuSIM test nodes (DU-CP and DU-UP) communicate through an internal network called the Keysight Internal Network.



The following table describes the settings for the KIN interface:

Setting	Description
<i>Start IP Settings - Select the Start IP address to open the Start IP configuration panel for editing.</i>	
IP Address	The IP address for the KIN Interface to use for traffic on this interface.
IP Prefix Length	The IP address prefix that has been assigned to the KIN Interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

Impairment Settings

Impairment is a Global setting that enables the deliberate insertion of anomalies into test network packet streams. By adding delays, drops, invalid flags, and so forth, you can evaluate how well your DUT responds to unexpected or malformed user plane or control plane traffic.

The following table describes the settings required to add and enable impairment in a test configuration.

Setting	Description
<i>Impairment Profiles:</i>	
	Click the Add impairment profile button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Click the Delete impairment profile button to remove the profile from your test configuration.
Name	Each impairment profile is uniquely identified by a name. You can accept the value provided by DuSIM or overwrite it with your own value.
Action Type	Select an option from the drop-down list: <ul style="list-style-type: none"> Custom script: Use this option to upload a custom Python script that executes the impairment actions. PFCP – Drop message: This option is not applicable in DuSIM.
Script file	If you have selected <i>Custom script</i> as the Action Type, select the Upload button to upload your custom Python script to the test configuration. To remove the script, select the Clear button.

The profiles that you add will be available when managing agents from the [Network Management on page 65](#) window.

Session Settings

The following table describes the settings of your test session, like controlling the length of the graceful shutdown process.

Setting	Description
Graceful Shutdown Enabled	Enable this option to allow for graceful shutdown of the test session.
Duration (s)	<p>Specify the global test duration (in seconds). This value specifies the duration of the entire test session, which includes all of the Scenario Groups for all of the Subscribers configured in the test. This duration setting takes effect regardless of the traffic <i>Duration</i> values defined in each of the Test Procedures configured in the Test Suites.</p> <p>Once this duration value is reached, DuSIM closes any open UE sessions and stops the test.</p>



DNNs Settings

In the 5G architecture, a Data Network Name (DNN) serves as the identifier for a data network. It is the equivalent of an APN (Access Point Name) in an LTE network. A DNN is used when selecting an SMF and UPF for a PDU session, selecting an N6 interface for a PDU session, and determining policies to apply to a PDU session.

The **DNN** panel contains the configuration settings for an individual DNN. In this panel, you can:

- Click the **Delete DNN** button to delete the DNN configuration.
- Edit the DNN settings.

The following table describes the DNN settings:

Setting	Description
<i>DNNs:</i>	
	Click the Add DNN button to add a new DNN to your test configuration.
<i>DNN:</i>	
	Click the Delete button to remove the DNN from your test configuration.
DNN	<p>Enter the DNN value for this DNN definition. For example: <code>dnn.keysight.com</code>.</p> <p>A DNN (as is the case with an EPS APN) is composed of two parts:</p> <ul style="list-style-type: none"> • A mandatory Network Identifier that defines the external network to which the UPF is connected.

Setting	Description
	<ul style="list-style-type: none"> An optional Operator Identifier that defines the PLMN backbone in which the UPF is located. <p>A 5GS Data Network Name (DNN) is equivalent to an EPS APN. It is a reference to a data network, and it may be used to select an SMF or UPF for a PDU session and to determine policies applicable to the PDU session.</p> <p>The DNN field supports dynamic values. These values can be obtained with a sequence generator. The sequence can be added anywhere in the DNN name (beginning, middle or end). The syntax is <code>[start_value-end_value,increment]</code>.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>NOTE The <code>start_value</code> and <code>end_value</code> must have the same length. For example, we can configure <code>dnn[008-999,1]</code> and obtain <code>dnn008,dnn009,...,dnn998,dnn999</code>. Syntaxes <code>dnn[8-999,1]</code> or <code>[008-1000,1]</code> are not valid as the start and end value lengths are different.</p> </div> <p>The start value is mandatory. Omitting certain parameters results in behaviors as exemplified below:</p> <ul style="list-style-type: none"> <code>dnn[4-9,]</code> an implicit increment of 1 is used <code>dnn[4-9]</code> as above <code>dnn[4-,1]</code> is used as <code>dnn[4-9,1]</code>, 9 being the maximum value with the configured length, length of 1 in this case <code>dnn[4-,]</code> as above <code>dnn[4-]</code> as above <code>dnn[4]</code> as above <p>UEs will use the DNN values from the pool in a round robin manner.</p> <div style="border: 1px solid black; padding: 5px; margin: 10px 0;"> <p>IMPORTANT If multiple sequence generators are configured and their pools overlap (for example: <code>dnn[000-600,1].keysight.com</code> <code>dnn[500-999,1].keysight.com</code>), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the <code>start_value</code> (they might start with an intermediate value in the second pool).</p> </div>
PDU Type	Select the desired PDU type: IPv4, IPv6, IPv4v6 or Ethernet.

MMW Settings

The MMW Settings provide one configuration option: *SCGAdd on PCELL only*, which is disabled by default.

This option controls the millimeter wave (MMW) mobility distribution logic such that the ScgAdd procedure will select only the primary serving cell (PCELL) of each DU during mobility events. As an example, if the option is enabled in a test in which there are four DUs that each have multiple cells, the MCG will select only the first cell of each DU (the PCell) during handovers. If the option is not enabled, the handovers can select other cells within each DU.



TM Settings

The following table describes the settings required for the Open RAN Simulators Cloud Edition Test Manager (TM) configuration.

Setting	Description
Subnet IPv6 Prefix	In static IPv6 configurations, you need to configure the network prefix for the UE's IP address. This is applicable when APN/DNN is IPv6 and Stateless Address Autoconfiguration (SLAAC) is not used to discover the network prefix.
5G NAS Attempt Counter	This is a Test Manager flag: it does not need to be modified.
Split Bearer	Enable this option if your NSA test needs split bearer functionality. When split bearer is enabled, a UE can simultaneously receive data from two paths: <ul style="list-style-type: none"> • One path is over the 5G air interface • The second path is over the X2 interface from the anchored eNodeB.
SCG Release using A2 Measurement	When this option is enabled in an NSA test scenario, DuSIM can release the secondary cell group (SCG) split bearer based on an A2 measurement that is reporting a lower UE signal. This occurs, for example, when a UE moves out of optimal cell coverage range, which results in a weak signal.

CA Certificates Settings

You use the CA Certificates global setting to upload one or more signed root CA certificate files for use in your test configuration. The following table describes these settings:

Setting	Description
<i>CA Certificates:</i>	
	Click the Add Certificate button to add a new IPsec certificate to your test configuration.
<i>CA Certificate:</i>	
	Click the Delete button to remove the selected certificate from your test configuration.
Name	Type in a unique name for the certificate.
Certificate File (.crt)	Do one of the following: <ul style="list-style-type: none"> • Select Upload to update a .crt file to your test configuration. • Select Clear to remove the .crt file from you test configuration.

CHAPTER 6

Assign and manage agents

A DuSIM *agent* is the virtual machine or docker container on which the application traffic and control plane procedure simulation is performed. Assigning and managing traffic agents is one of the essential and required aspects of creating and executing DU simulation tests.

Chapter contents:

About traffic agents	59
Assigning agents to nodes	60
Agent management	62
Network Management	65

About traffic agents

DuSIM tests require the use of *agents* to generate traffic for both DU-UP (user plane) and DU-CP (control plane). The containers and virtual machines that act as agents can be horizontally scaled to support a very high level of application traffic throughput and control plane procedure rates.

Agent implementation

Agents are implemented as containers or virtual machines, depending upon the platform on which they are deployed.

Platform	Supported platforms	Implementation
Public clouds	Amazon Web Services (AWS)	virtual machines
Private clouds	VMware ESXi 6.5 and ESXi 6.7	virtual machines
Servers	Kubernetes with OpenShift, Flannel, and Calico	Container

Assigning tags to agents

Tags provide a flexible and simple method of assigning metadata to agents. There are two types of tags:

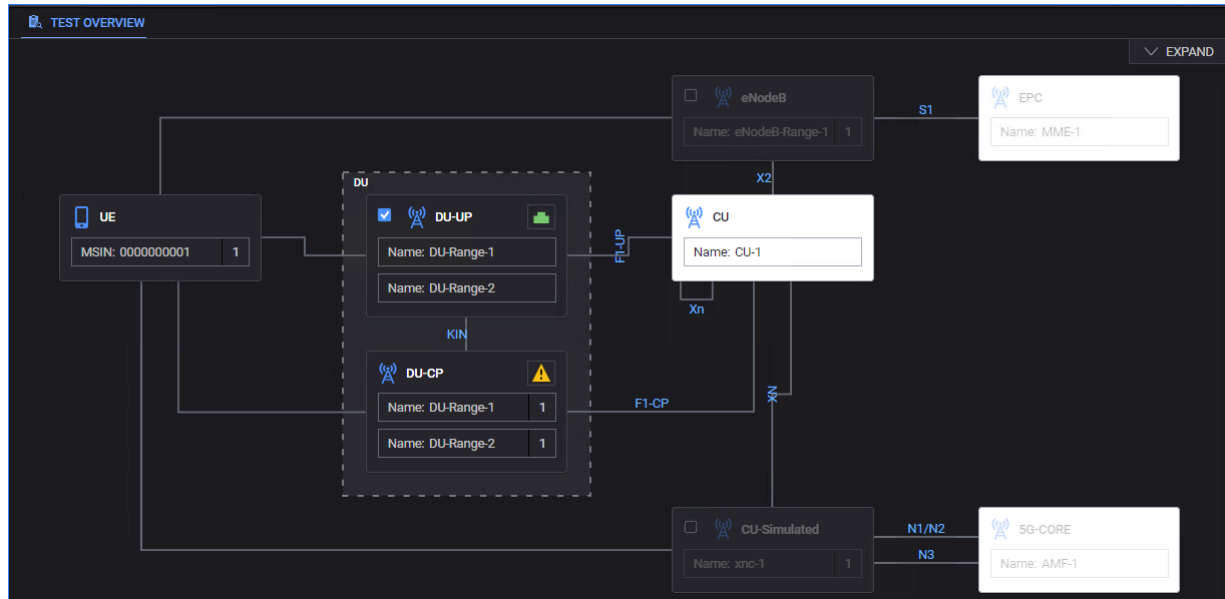
Type	Color	Description
System tag	Blue	These tags are defined by DuSIM. You can hover over the system tag icon to display the tag information.
User-defined tags	Gray	You can add custom tags from the Agent Management window. These are tags that you create; they are free-form, which gives you the ability to categorize or mark agents in any way that supports your test requirements. Refer to Agent management on page 62 for instructions.

Assigning agents to nodes



You cannot run a DuSIM test until you have assigned agents to all of the test nodes. To assign an agent to a node:

1. In the topology window, select the traffic agent icon on the top right corner of the node.

For example:



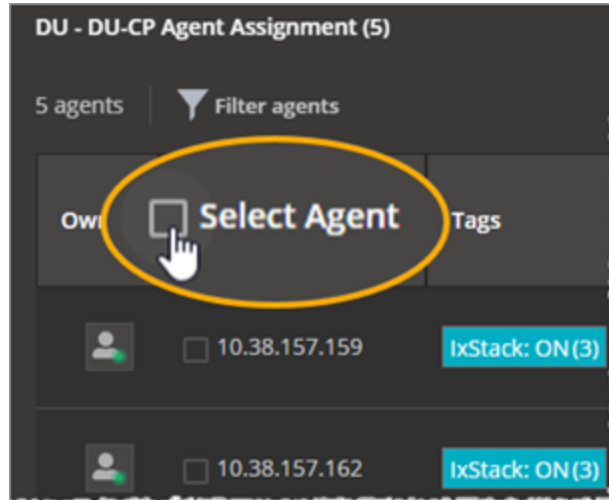
The icon that represents the agent can be any of the following:

-  — No agents are assigned to the node.
-  — One or more agents are assigned.

DuSIM opens the **Agents Assignment** window, which presents a list of agents. If the list has no filters set, then all agents are listed.

2. Assign specific agents or all available agents to the node:
 - To assign specific agents (one or more) to the node, select the check-box next to the agent's IP address.

To assign all available agents to the node, select the **Select Agent** check-box (located in the table header).



Note that you can display the agent ID by hovering over the IP address.

3. Select the F1 and KIN **Connections**, if required.
4. Click **Update**.

Agent Assignments window

The following table describes the content of each column displayed on the **Agents Assignment** window.

Column	Description
Owner	<p>Hover over the Owner icon to see the current agent ownership and status, which will be one of the following:</p> <ul style="list-style-type: none"> The agent is owned by the user whose email address is listed. In this case, the agent is not available for assignment. The agent is offline. In this case, the agent is not available for assignment. The agent is available for assignment.
Select Agent	<p>Use the check box next to the IP address to select that agent for assignment. You can also select all available agents by selecting the Select Agent check box (in the table header).</p>
Tags	<p>This column displays the tags associated with each agent. Each tag indicates the number of agents to which it is associated.</p> <p>Refer to About traffic agents on page 59 for more information about tags.</p>
Connections	<p>The table displays the available interface and the MAC address for each wireless connection. The interface can be selected from the drop-down list.</p> <div style="display: flex; align-items: flex-start;"> <div style="background-color: #f0f0f0; padding: 5px; margin-right: 10px; text-align: center;">NOTE</div> <div> <p>For the DuSIM nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.</p> </div> </div>

NOTE

From the **Agents Assignment** window you can select other nodes from the list and configure the agents for those nodes also. In this way, you can configure agents for all your test nodes at the same time.

Agent management

You manage your DuSIM agents from the **Agent Management** window, which is accessed from the Setting menu (⚙️). This window displays detailed information for all or selected agents and provides all of the functionality needed to manage them.

- [Agent Management window below](#)
- [Selecting agents on the next page](#)
- [Search, select, and filter agent data on the next page](#)
- [Adding and removing tags on the next page](#)
- [Agent management actions on page 64](#)

Agent Management window

The Agent Management window displays a table that shows the current status of your agents.

Column	Description
<input type="checkbox"/>	<p>The first column in the table contains a checkbox that you use when selecting individual agents for various operations.</p> <p>Note that you can use the <i>Agent IP</i> checkbox in the table header to select all agents.</p>
Agent IP	<p>Displays the IP address of the agent.</p> <p>To see the Agent ID, hover over the agent's IP IP address.</p>
Owner	Indicates whether the agent is assigned, available, or offline.
Status	Indicates the current status of the agent.
Tags	<p>This column displays the tags associated to each agent.</p> <p>There are two types of tags:</p> <ul style="list-style-type: none"> • system tags (blue): these are defined by DuSIM. You can hover over a system tag to view more details. • user tags (gray): these are defined by dusim users. Refer to Adding and removing tags on the next page for more details. <p>Each tag indicates the number of agents to which it was associated.</p>
Test NICs	Displays the NICs for each agent and, on hover, it displays the MAC address.
Hostname	Displays the hostname.
Memory	Displays the amount of RAM memory allocated to the agent.
CPU info	Displays additional information about the CPU model, the frequency and the

Column	Description
	number of cores.
Last Run Data	Displays the nodes that were last run on the agent.
Last Run Timestamp	Displays the date and time of the last agent run.

Selecting agents

You can perform management actions on individually-selected agents (one or more) or on all agents:

- To select a specific agent, select the check-box associated with the agent's IP address. (When hovering over the IP address of an agent, the agent ID is displayed.)
- To select all agents currently listed in the table, select the *Agent IP* checkbox in the table header.

Search, select, and filter agent data

You can selectively locate and display agent data using the following functions:

Function	Description
Filter agents	<p>Use this option to filter the available agents by tag names:</p> <ol style="list-style-type: none"> 1. Select Filter agents. 2. Enter the name of the tag or select it from the available list. 3. Select Close. <p>The content on the Agent Management window is updated with the filtering results.</p> <p>To remove the filtering results, select Clear.</p>
Include offline agents	Set this option to either include or exclude offline agents from the list.
Search	Search by IP, Owner, hostname, or status.

Adding and removing tags

You can create and use tags to categorize agents in any way that suits your needs.

Add a custom tag:

1. Select one or more agents in the table.
2. Select **Tag as**.
3. Type the name of the tag in the **Search or add tag** field, then select **Add**.
4. Select **Update** to add the tag name.

Remove a tag:

1. Select one or more agents in the table.
2. Select **Tag as**.
3. Select **Remove tags**.
4. Use the search functionality to identify the tag name or select it from the list.
5. Select **Update** to remove the tag name.

Agent management actions

You can perform the following actions on the agents that are currently selected (selected via the selection checkbox in the first column of the table):

Function	Description
Clear ownership	Releases your ownership of the selected agents.
Hard reboot	Performs a hard reboot on the agent (the agent machine is power-cycled).
Delete	Removes the selected agent(s) from the Agent Management list.

Network Management

All of the agents selected in the **Agents Assignment** window are displayed on the **Network Management** window.

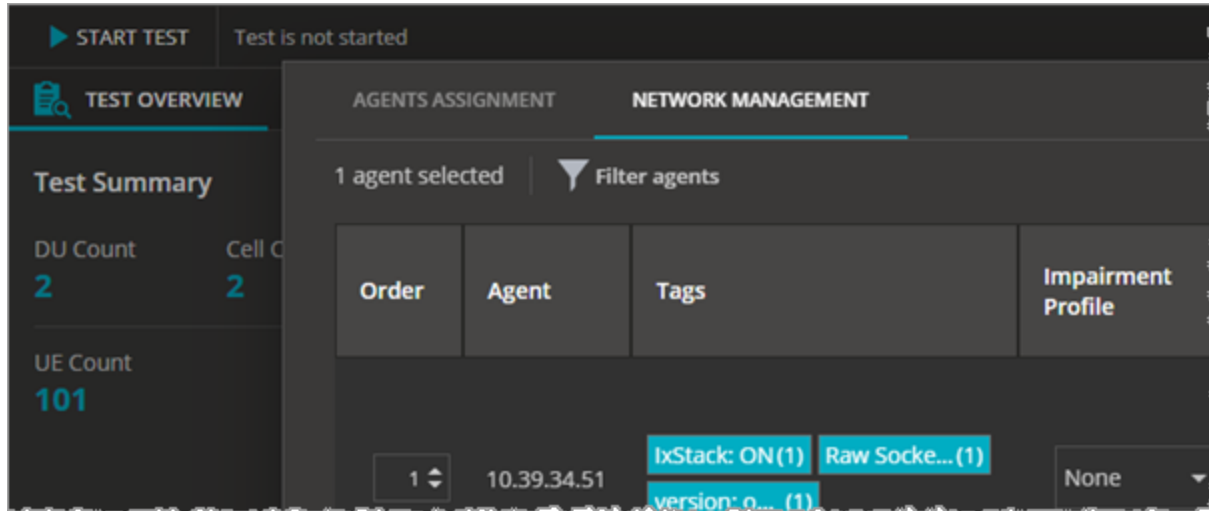


Table description

The following table describes the content of each column displayed on the **Network Management** window.

Column	Description
Order	This option allows you to select the agent distribution order when running with multiple agents on the same node (when you are not using a switch to connect all agents).
Agent	Displays the agent's IP address. When hovering over the IP address of the agent, the agent ID is displayed.
Tags	<p>This column displays the tags associated to each agent.</p> <p>There are two types of tags:</p> <ul style="list-style-type: none"> system tags (blue): these are defined by DuSIM. You can hover over a system tag to view more details. user tags (gray): these are defined by dusim users. Refer to Adding and removing tags on page 63 for more details. <p>Each tag indicates the number of agents to which it was associated.</p>
Impairment profile	Allows you the select an impairment profile from the drop-down list.
Agent Interface	Displays the agent's interface Name and MAC address.

Column	Description
Network Stack	<p>This option allows you to select the network stack used to run the test:</p> <ul style="list-style-type: none"> • Linux Stack • IxStack over Raw Sockets • IxStack over DPDK <p>An agent compatible with IxStack is marked using an <code>IxStack: On/Off</code> system tag.</p>
SRIoV	<p>This option is disabled when <i>Network Stack</i> is set to Linux Stack. For IxStack over Raw Sockets or IxStack over DPDK, this option is enabled based on the selection (it can be enabled or disabled based on your agent's configuration).</p>
Traffic Capture	<p>This option allows you to enable or disable traffic capture on all or specific interfaces, based on your test configuration.</p>
Entity	<p>Displays the nodes on which the agent has been assigned. When hovering over the node, it displays the node's interface names.</p>

IMPORTANT

To run tests using IxStack over Raw Sockets or IxStack over DPDK you need at least two agents.

Filtering agents

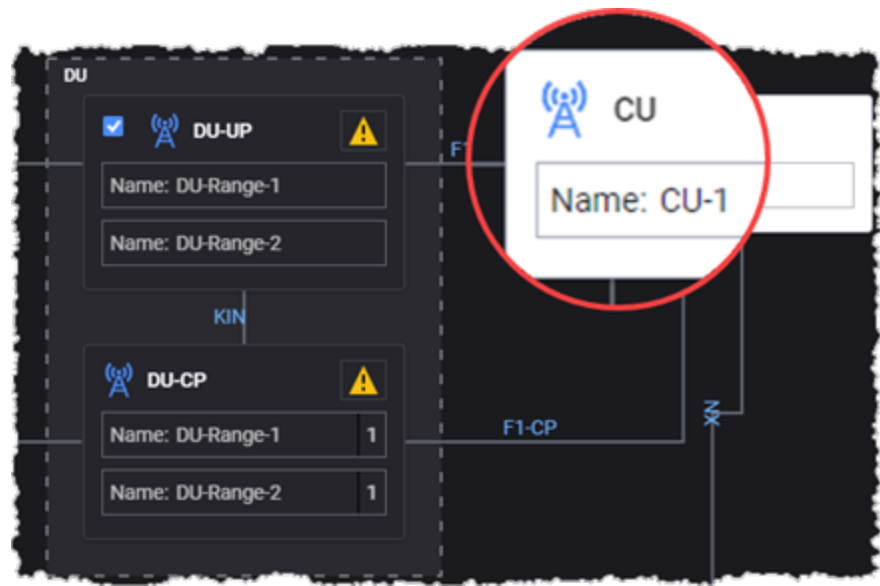
You can set filters (using tag names) to determine which agents are displayed in the table:

1. Select **Filter agents**.
2. Enter the name of the tag or select it from the available list.
3. Select **Close**.

The content on the **Network Management** window is updated to show only agents that are tagged with one of the tags selected in your filter setting.

CHAPTER 7

CU configuration settings



The gNB Central Unit (CU) is responsible for MC (mobility control), RRM (Radio Resource Management) and SM (Session Management). It hosts RRC, SDAP, and PDCP protocols of the gNB that controls the operation of one or more gNB-DUs. The gNB-CU terminates the F1 interface connected with the gNB-DU.

The CU is the device under test (DUT) in a Keysight DuSIM test configuration.

Chapter contents:

CUs panel	68
CU panel	68
F1-C Interface Settings	70
X2-C Interface Settings	70
Xn-C Interface Settings	71
F1-U Interface Settings	72

CUs panel

The **CUs** panel opens when you select the CU node from the network topology window. You can perform the following tasks from this panel:

- Add a new CU range to your test configuration.
- Open a CU range configuration for editing or viewing.
- Enable or disable a range for the test session.

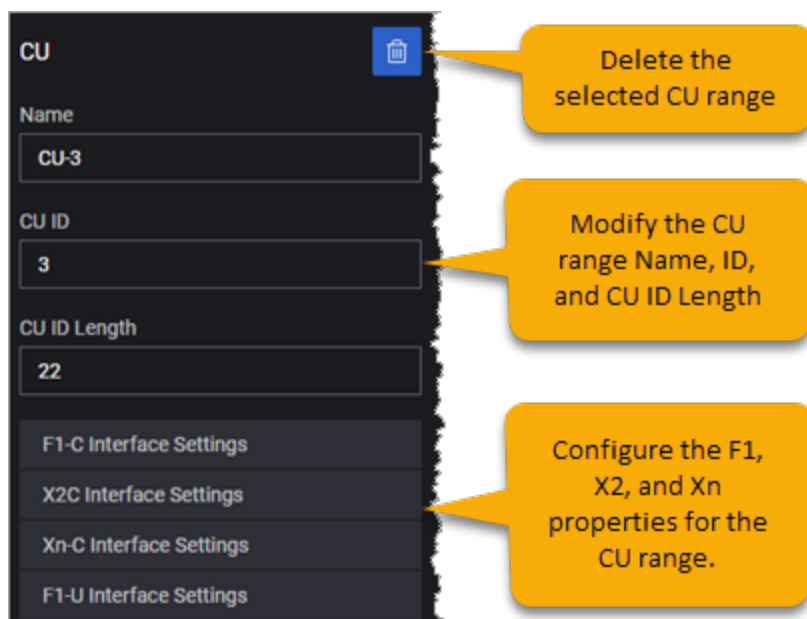
For example ...



CU panel

When you select a node from the **CUs** panel, DuSIM opens the **CU** panel, from which you can:

- Select the **Delete** button to delete the selected CU range from the test configuration.
- Modify the CU range name, CU ID, and CU ID length.
- Select each of the **Interface Settings** to configure the connectivity settings for the CU range.



CU Identification settings

You can add multiple CUs in your test network. The following settings provide a unique identification for each of them.

Setting	Description
Name	Keysight Open RAN Simulators, Cloud Edition 3.0 creates a default name for each CU in the test topology. You can change the names to give a more specific identification to each of them.
CU ID	The gNB-CU Identifier (which is part of the NR Cell Identity). The valid value range is from 0 to 4,294,967,295.
CU ID Length	The length (number of bits) of the CU ID. The ID can be configured to use between 22 bits and 32 bits.

CU Interface Settings

Each CU range provides IP and/or IPsec settings for the following interfaces:

F1-C Interface Settings	70
X2-C Interface Settings	70
Xn-C Interface Settings	71
F1-U Interface Settings	72

F1-C Interface Settings

You access the F1-C Interface Settings from a CU range panel ([CU panel on page 68](#)). The F1-C interface carries signaling packets between the CU and DU nodes.

IP

The following table describes the F1-C interface IP settings.

Setting	Description
IP Address	Enter the IP address for the CU F1-C interface.
IP Prefix Length	The subnet prefix length associated with this IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	This DU-CP node's gateway address.

IPsec

The following table describes the F1-C interface IPsec settings. To enable IPsec on this interface, the CU needs only the IP address, prefix, and port number of the client-side IPsec tunnel. Refer to [F1-CP Interface Settings on page 80](#) for the client-side IPsec configuration settings.

Setting	Description
Source Port	The IPsec tunnel's source port.
IP Address	The IP address of the F1-C IPsec interface on the CU range.
IP Prefix Length	The IP address subnet prefix length associated with this IPsec interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

X2-C Interface Settings

You access the X2-C Interface Settings from a CU range panel ([CU panel on page 68](#)). The X2-C interface carries signaling packets between RAN nodes in non-standalone (NSA) operations.

IP

The following table describes the X2-C interface IP settings.

Setting	Description
IP Address	Enter the IP address for the CU X2-C interface.
IP Prefix Length	The subnet prefix length associated with this IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

Setting	Description
Port	The port associated with this interface.
Gateway Address	This CU node's gateway address.

IPsec

The following table describes the X2-C interface IPsec settings. To enable IPsec on this interface, the CU needs only the IP address, prefix, and port number of the client-side IPsec tunnel. Refer to [X2-C Interface Settings on page 100](#) for the client-side IPsec configuration settings.

Setting	Description
Source Port	The IPsec tunnel's source port.
IP Address	The IP address of the X2-C interface on the CU range.
IP Prefix Length	The IP address subnet prefix length associated with this IPsec interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

Xn-C Interface Settings

You access the Xn-C Interface Settings from a CU range panel ([CU panel on page 68](#)). Xn is a network interface between NG-RAN nodes: specifically, between gNB-gNB, between (gNB)-(ng-eNB) and between (ng-eNB)-(ng-eNB). Xn-U is used for the Xn User Plane interface, and Xn-C is used for the Xn Control Plane

IP

The following table describes the Xn-C interface IP settings.

Setting	Description
IP Address	Enter the IP address for the CU Xn-C interface.
IP Prefix Length	The subnet prefix length associated with this IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Port	The port associated with this interface.
Gateway Address	This CU node's gateway address.

F1-U Interface Settings

You access the F1-U Interface Settings from a CU range panel ([CU panel on page 68](#)). The F1-U interface carries data packets between the CU and DU nodes.

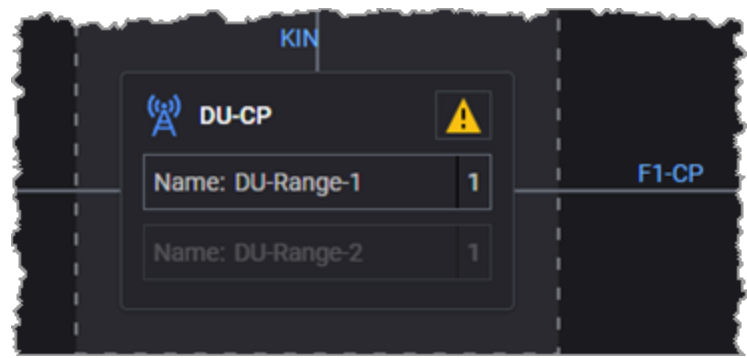
IPsec

The following table describes the F1-U interface IPsec settings. To enable IPsec on this interface, the CU needs only the IP address, prefix, and port number of the client-side IPsec tunnel. Refer to [DU-UP Range panel on page 90](#) for the client-side IPsec configuration settings.

Setting	Description
Source Port	The IPsec tunnel's source port.
IP Address	The IP address of the F1-U IPsec interface on the CU range.
IP Prefix Length	The IP address subnet prefix length associated with this IPsec interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

CHAPTER 8

DU-CP configuration settings



The gNB Distributed Unit (gNB-DU) is a logical node hosting RLC, MAC, and PHY layers of the gNB, and its operation is partly controlled by a gNB-CU. One gNB-DU supports one or multiple cells, and it terminates the F1 interface connected with the gNB-CU.

In the DuSIM test topology, the gNB-DU is logically structured as two entities:

- DU-CP, which connects with the CU over the F1-C interface, which carries control plane traffic.
- DU-UP, which connects with the CU over the F1-U interface, which carries user plane traffic.

The chapter describes the **DU-CP** settings.

Chapter contents:

DU-CP Range panel	74
DU-CP RANGE panel	75
Cells settings	77
Measurement Timing Configuration	79
F1-CP Interface Settings	80
DU-PROCEDURE RANGE panel	86

DU-CP Range panel

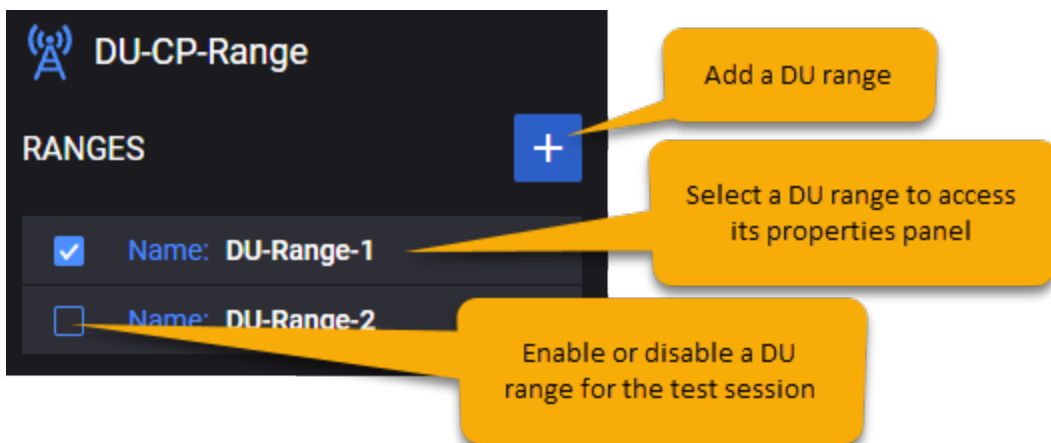
The **DU-CP Range** panel opens when you select the DU-CP node from the network topology window. It enables the creation of DU-CP ranges and also DU Procedure ranges.

DU node ranges

You can perform the following tasks from the **Ranges** section of the panel:

- Add a new DU range to your test configuration.
- Open a DU range configuration for editing or viewing.
- Enable or disable a range for the test configuration.

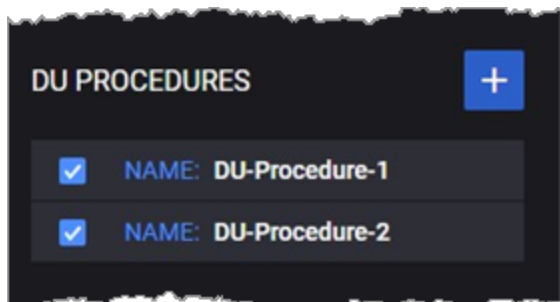
For example ...



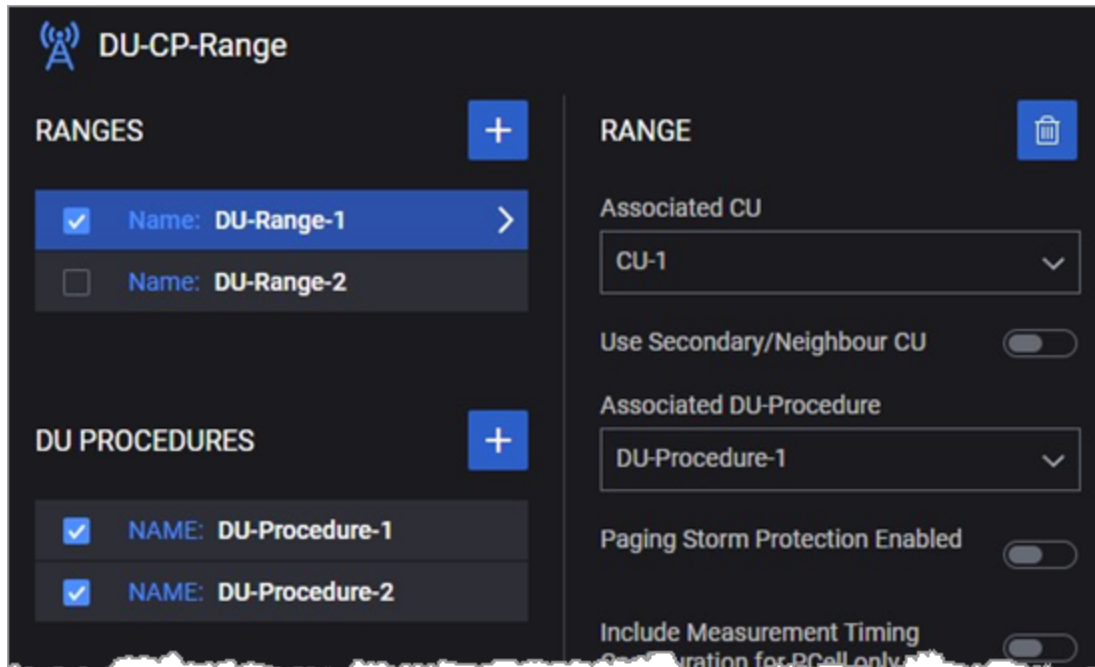
DU Procedure ranges

You use the DU Procedure ranges to configure DU failure scenarios. Once you have configured a failure scenario, you can select it in your DU-CP Range settings (which are describe in [DU-CP RANGE panel on the facing page](#)).

As with the DU-CP ranges, you can add, select, and enable or disable these ranges from the DU-CP Range panel.



DU-CP RANGE panel



When you select a DU-CP range from the **DU-CP Range** panel, DuSIM opens the **RANGE** panel, from which you can:

- Select the **Delete** button to delete the selected DU-CP range from the test configuration.
- Configure the settings for the selected DU-CP range.

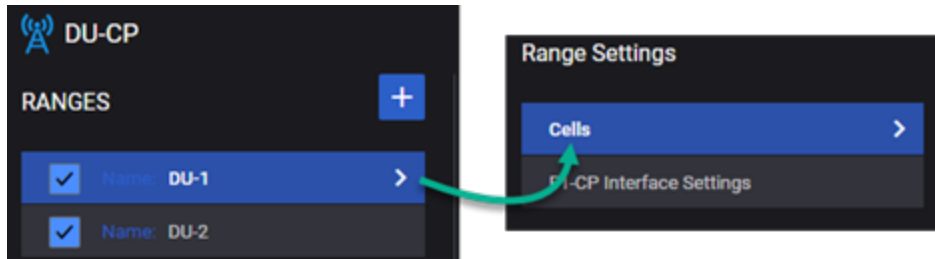
The following table describes the available settings that are required for each DU-CP range.

Setting	Description				
Associated CU	Select the gNB CU range that controls this DU-CP range.				
Use Secondary/Neighbor CU	<p>Select this option to enable inter-CU handovers. (Refer to the <i>Strategy</i> setting in Mobility settings on page 172 for more information about handover types.)</p> <p>When you select the option, the panel displays two additional configuration options:</p> <table border="1"> <tr> <td>Secondary/Neighbour CU:</td><td>Select the CU node to act as the secondary CU; this is the CU that will accept handovers from the primary CU (which is selected in the <i>Associated CU</i> setting).</td></tr> <tr> <td>Use Secondary/Neighbour CU First:</td><td>When you enable this option, UEs that are attached to the <i>Associated CU</i> will handover to the Secondary/Neighbour</td></tr> </table>	Secondary/Neighbour CU:	Select the CU node to act as the secondary CU; this is the CU that will accept handovers from the primary CU (which is selected in the <i>Associated CU</i> setting).	Use Secondary/Neighbour CU First:	When you enable this option, UEs that are attached to the <i>Associated CU</i> will handover to the Secondary/Neighbour
Secondary/Neighbour CU:	Select the CU node to act as the secondary CU; this is the CU that will accept handovers from the primary CU (which is selected in the <i>Associated CU</i> setting).				
Use Secondary/Neighbour CU First:	When you enable this option, UEs that are attached to the <i>Associated CU</i> will handover to the Secondary/Neighbour				

Setting	Description
	<div></div> CU.
Associated DU-Procedure	An Associated DU-Procedure is mandatory for all DU-Ranges. It is mapped to a corresponding "DU-Procedure-Range" (which you select from the drop-down list) to specify which "DU-Procedure-Range" settings will be used for that particular DU-Range. See also, DU-PROCEDURE RANGE panel on page 86 .
Paging Storm Protection Enabled	Select this option to protect the DU-CP from paging storms (a surge in paging requests over a short time period).
Include Measurement Timing Configuration for PCell only	This IE is reported for PCell only when this flag is enabled.
Include DU System Information	When this flag is enabled, the gNB-DU System Information IE that includes MIB and SIB messages is included in the F1 Setup Request message.
Include 5GS TAC	This flag controls the 5GS-TAC optional IE presence in the F1 Setup Request message (the IE identifies the Tracking Area Code). When disabled, the IE is not included.
DU Latest RRC Version	The Latest RRC Version IE is part of gNB-DU RRC version IE in the F1 Setup Request message. Decimal user input is encoded in a 3-bit field in the F1 Setup message.
DU ID	Enter the gNB-DU ID for this DU-CP range. The gNB-DU ID uniquely identifies the gNB-DU within a gNB-CU. It is provided to the gNB-CU during the F1 Setup procedure, and is used only within F1AP procedures.
DU ID Length	The number of bits (from the NRCGI) to use for the DU ID. (The number of bits to use for the DU ID is a vendor decision.)
Range Count	By default, a DU-CP range contains one DU-CP node. If you want to create multiple DU-CP nodes for the range, enter the desired number in this field.
<i>Range Settings:</i>	
Cells	Refer to Cells settings on the facing page .
F1-CP Interface	Refer to F1-CP Interface Settings on page 80 .

Cells settings

Each **DU-CP** range requires configuration of a group of **Range Settings**, which include the range's **Cells** settings.



These settings are organized in the following groups:

- [Cells below](#)
- [NSSAI on the next page](#)
- [Cells Settings on the next page](#)



Cells

Each DU-CP range requires configuration of a group of **Cells** settings, which are the cells that this gNB-DU supports:

Setting	Description
Cell ID	The NR Cell Global Identifier (NRCGI) for this DuSIM range.
Cell ID Increment	Enter the value by which DuSIM will increment each <i>Cell ID</i> if the <i>Cell Count</i> is greater than 1.
Cell Count	Each DU can have multiple cells. If you want to create multiple cells for the DU-CP range, enter the desired number in this field.
NR Sub Carrier Spacing	Select the subcarrier spacing value for the served cell. In 5G networks, the subcarrier spacing scales by $2\mu \times 15$ kHz to cover different services: QoS, latency requirements, and frequency ranges. 15, 30, and 60 kHz subcarrier spacing are used for the lower frequency bands, and 60, 120, and 240 kHz subcarrier spacing are used for the higher frequency bands.
PLMN Identity	The Public Land Mobile Network (PLMN) in which this cell is located. The PLMN is a globally unique identifier that comprises the MCC and MNC: <ul style="list-style-type: none"> • PLMN MCC: The PLMN's mobile country code (MCC). • PLMN MNC: The PLMN's mobile network code (MNC).
Measurement Timing Configuration	Refer to Measurement Timing Configuration on page 79 for a description of the configuration settings.

NSSAI

Each DU-CP range requires configuration of a group of **NSSAI** settings, which are described in the following table:

Setting	Description
	The following actions are available: <ul style="list-style-type: none"> Select the Add NSSAI button to add a new NSSAI to your test configuration. Select UE NSSAI from the list to access the configuration settings.
<i>NSSAI panel:</i>	
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.
SST	The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the S-NSSAI information element. The standardized SST values are: <ul style="list-style-type: none"> 1 (eMBB) 2 (URLCC) 3 (MIoT)
SD	The Slice Differentiator (SD) value for this NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The Mapped configured Slice/Service Type (SST) value for this NSSAI.
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this NSSAI.

Cells Settings

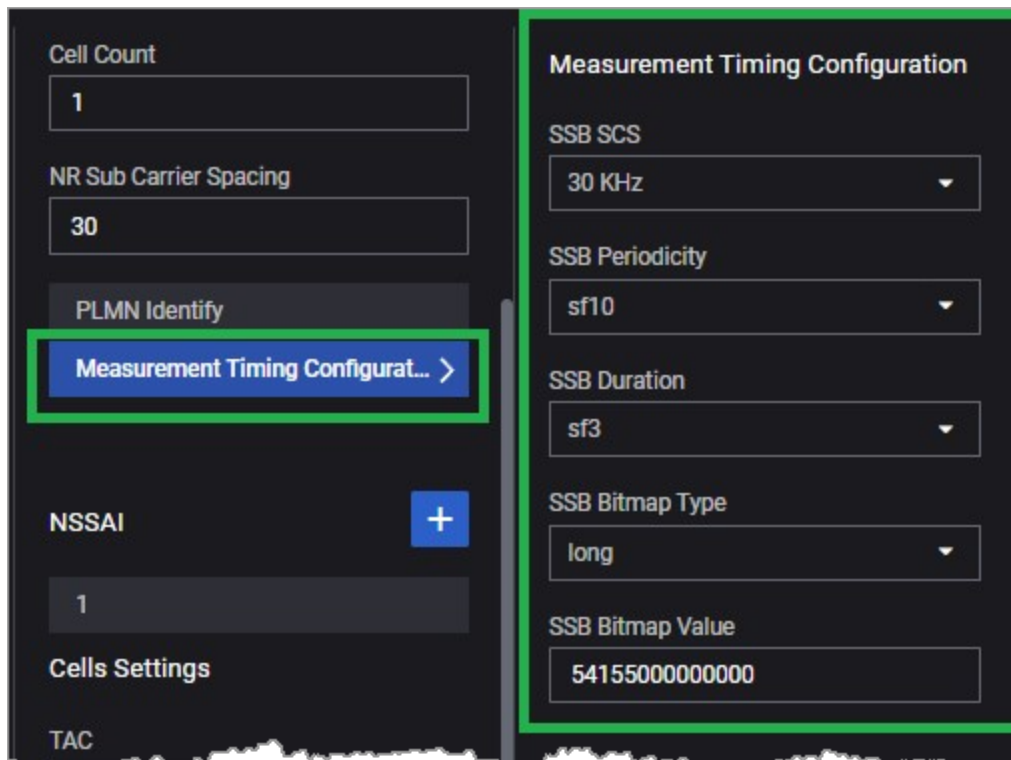
Each DU-CP range requires configuration of a group of **Cells Settings** settings, which are described in the following table. These value are used by each of the cells defined in this DU-CP range.

Setting	Description
TAC	The unique identifier of the Tracking Area Code (TAC) to which this cell belongs in the 5G system.
DL-NR-ARFCN	Enter the desired downlink NR-ARFCN code for this cell range.
UL-NR-ARFCN	Enter the desired uplink NR-ARFCN code for this cell range.
NR Band	The NR Frequency Band for this cell.

Setting	Description
	The default value is 11, the minimum is 1, and the maximum is 261. These correspond to the n1, n2, ..., n261 band designations.
SSB ARFCN	Set this value to match the NR SSref (SSB) ARFCN value that is configured in the DUT.
ARFCN POINTA	The ARFCN NR Reference Point A value. Set this value to match the value that is configured in the DUT.
NRNRB	NRNRB is one of the enumerated values (nrb11, nrb18, nrb24, ...) in the NR-Mode-Info IE. This IE value reflects in NR Mode Info of the gNB DU's served cell information in the F1 Setup message.

Measurement Timing Configuration

Each DU-CP range requires measure timing configuration, as part of the Cells configuration. To access the configuration panel, select **Measurement Timing Configuration** from the **Cells** panel.



This Optional IE is included in the F1 Setup procedure for simulated Cells. It contains the MeasurementTimingConfiguration inter-node message defined in TS 38.331.

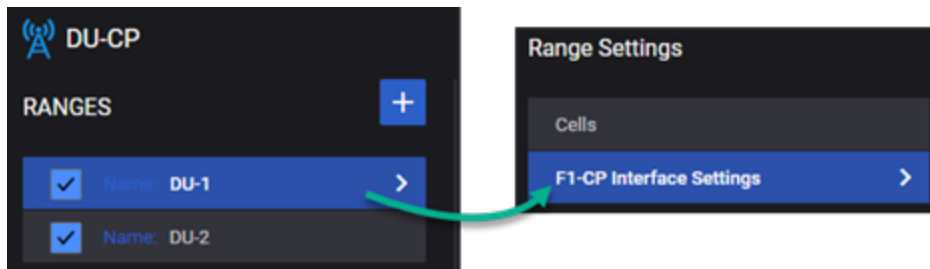
The following table describes the configuration settings.

Setting	Description
SSB SCS	Select the desired Synchronization Signal Block (SSB) Subcarrier Spacing (SCS)

Setting	Description
	from the drop-down list.
SSB Periodicity	Select the desired <i>periodicityAndOffset</i> value from the drop-down list.
SSB Duration	Select the desired <i>duration</i> parameter from the drop-down list.
SSB Bitmap Type	Select the desired value of <i>ssb-ToMeasure</i> from the drop-down list. The SSB-ToMeasure IE is used to configure a pattern of SSBs. Possible values are shortBitmap, mediumBitmap, and longBitmap.
SSB Bitmap Value	Based on the <i>ssb-ToMeasure</i> bitmap type selected, input a corresponding bitmap value.

F1-CP Interface Settings

Each **DU-CP** range requires configuration of a group of **Range Settings**, which include the range's **F1-CP Interface Settings**.



These settings enable communication between the simulated DUs and your DUT. They are organized as follows:

- [F1 interface Settings below](#)
- [Connectivity Settings on the facing page](#)

F1 interface Settings

The F1-CP interface settings specify the F1 port number and the interface setup wait time.

Setting	Description
F1 Port	The port to use for the F1 connection. The default port number is 38472, which is an unassigned IANA port number. You can set this to a different value, if appropriate for your test requirements.
F1 Setup Wait Time (ms)	The amount of time (in milliseconds) that DuSIM will wait before establishing the connection on the F1 interface.
F1 Setup Request	The amount of time (in milliseconds) to delay sending the F1 Setup Request message to the gNB-CU.

Setting	Description
Delay (ms)	This option is available only when IPsec is enabled.

Connectivity Settings

The F1-CP connectivity settings are organized into the following groups:

- [F1C IP Connectivity Settings below](#)
- [VLAN settings below](#)
- [IPsec settings on the next page](#)

F1C IP Connectivity Settings

These settings specify the F1-CP IP settings.

Setting	Description
IP Address	Enter the IP address that the first DuSIM DU node defined in this range will use to communicate with the gNB-CU (device under test).
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the DU-CP nodes that are defined in this range will be incremented. The number of IP addresses that will be created is determined by the <i>Range Count</i> RANGE value.
IP Prefix Length	The subnet prefix length associated with this IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	This DU-CP node's gateway address.

VLAN settings

The following VLAN settings are available for the DU-CP F1 interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

IPsec settings

The following IPsec settings are available for the DU-CP F1 interfaces.

Setting	Description
Destination Port	The IPsec tunnel's destination port.
Source Port	The IPsec tunnel's source port.
IP	The IP address of the F1-C interface on the DU range.
Role	<p>The role that this interface will play in the test:</p> <ul style="list-style-type: none"> • Initiator (Site-to-Site): The node will function as the initiator in the test (will initiate the tunnels). This option is used for site-to-site tests. • Initiator (Remote Access): The node will function as the initiator in the test (will initiate the tunnels). This option is used for Remote Access scenarios, in which an individual client is connected to a LAN through a secure tunnel. In this scenario, the client is operating as its own Secure Gateway. <p>The default value is <i>Initiator (Site-to-Site)</i>.</p>
<i>IPsec Authentication settings:</i>	
Authentication Method	<p>Select the authentication method to use in this configuration. The options are:</p> <ul style="list-style-type: none"> • Certificates: Use CA certificates for authentication. • Pre-Shared Key: Use a pre-shared key rather than certificates.
CA Certificate	<p>Select a CA certificate that you have previously uploaded. Uploading certificates is managed in the DuSIM Global settings. Refer to CA Certificates Settings on page 57 for instructions.</p>
Certificate and Private Keys	<p>To upload a zip file that contains the certificate file (extension .crt) and the private key (extension .key):</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Upload. <p>Note that the two files contained in the zip file should have the same file name (such as cert10.crt and cert10.key).</p> <p>To remove a zip file that has been previously uploaded:</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Clear.
Use Same Certificate and Private Key for all Instances	<p>Use the uploaded certificate and key file for all test instances of this configuration.</p>

Setting	Description
<i>IPsec IKE Phase 1 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
DH Group	<p>Specifies the Diffie-Hellman (DH) Group.</p> <p>The DH key exchange algorithm allows two parties to jointly establish a shared secret key over an insecure communications channel. DH groups determine the strength of the key used in the key exchange process. The higher the group number, the more secure the key. For example, DH group 1 is a 768-bit group and DH group 2 is a 1024-bit group.</p>
PRF Algorithm	<p>Specifies the algorithm used to perform Pseudo-Random Functions (key derivations).</p> <p>The PRF choices are...</p> <ul style="list-style-type: none"> • HMAC-MD5: Hash-based Message Authentication Code, Message-Digest Algorithm 5. • HMAC-SHA1: Hash-based Message Authentication Code, Secure Hash Algorithm 1. • HMAC-SHA256: Hash-based Message Authentication Code, Secure Hash Algorithm 256. • HMAC-SHA384: Hash-based Message Authentication Code, Secure Hash Algorithm 384. • HMAC-SHA512: Hash-based Message Authentication Code, Secure Hash Algorithm 512.
<i>IPsec IKE Phase 2 settings:</i>	
Encryption Algorithm	Specifies the encryption algorithm used to protect communications during message exchanges.

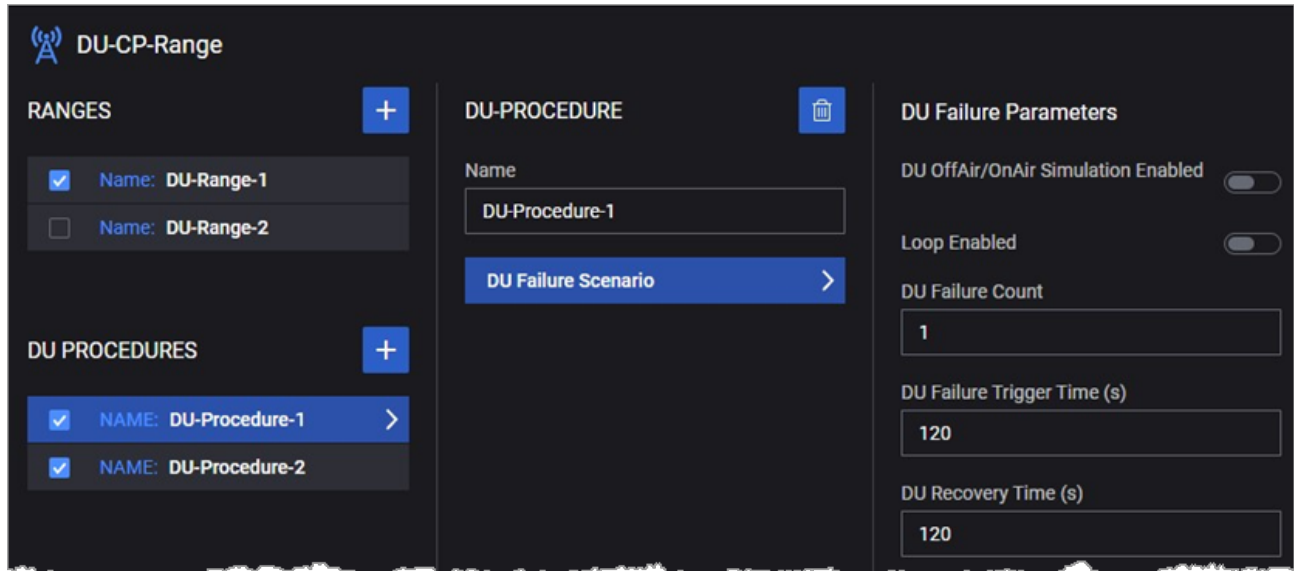
Setting	Description
	<p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
<i>IPsec Identification settings:</i>	
Local Identification Type	<p>The Identification Type field describes the type of information contained in the IPsec packet Identification Data field. See RFC 2407 for more information.</p> <p>The choices are...</p> <ul style="list-style-type: none"> • ID_IP_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as a single four-octet IPv4 address. • ID_FQDN: Sets the Identification Type field to 2 and inserts the gateway address into the Identification Data field as a fully-qualified domain name string. For example, "foo.bar.com". • ID_USER_FQDN: Sets the Identification Type field to 3 and inserts the gateway address into the Identification Data field as a fully-qualified username string. For example, "piper@foo.bar.com". • ID_Iv6P_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as an IPv6 address. • ID_DER_ASN1_DN: Sets the Identification Type field to 9 and inserts the gateway address into the Identification Data field as a binary DER encoding of an ASN.1 X.500 Certificate Distinguished Name. • ID_KEY_ID: Sets the Identification Type field to 11 and inserts the gateway address into the Identification Data field as an opaque byte stream that may be used to pass vendor-specific information necessary to identify which pre-shared key should be used to authenticate Aggressive mode negotiations. ID_KEY_ID is recommended for Network Access Identifiers (NAIs) that do not include the realm component (reference: draft-eronen-ipsec-ikev2-clarifications). ID_KEY_ID is supported by IKEv2 only.
Local	The Local Identification Value is a string value, with a maximum of 1024

Setting	Description
Identification Value	characters.
<i>IPsec Timers settings:</i>	
Enable Rekey	<p>Enables or disables renegotiation of Phase 1 and Phase 2 SAs on expiry of tunnel lifetimes:</p> <ul style="list-style-type: none"> • When disabled, tunnels are torn down when their lifetimes expire. • When enabled, the tunnels' Phase 1 and Phase 2 options are renegotiated before their lifetimes expire, and the tunnels stay up.
IKE Phase 1 (IKE) Lifetime	<p>Specifies the Phase 1 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.</p>
IKE Phase 2 (ESP) Lifetime	<p>Specifies the Phase 2 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.</p>
DPD Interval	<p>When this value is set to a value greater than zero, each IKE peer in the range uses the Dead Peer Detection (DPD) protocol to determine proof of liveness of the other peer. The peers send DPD HELLO messages according to the interval that you specify.</p> <p>When the value is set to zero, the IKE peers do not send DPD HELLO messages.</p> <p>An IPsec endpoint uses DPD to confirm that its peer is still up. DPD is implemented in IKE through the use of an asynchronous, bidirectional message exchange:</p> <ul style="list-style-type: none"> • DPD HELLO • DPD HELLO ACK <p>A complete DPD exchange (transmission of DPD HELLO and receipt of the corresponding DPD HELLO ACK) serves as proof of liveness. If a node does not receive a response to a DPD HELLO within a specified time, it assumes that the peer is dead or unreachable, and tears down the tunnel.</p>

DU-PROCEDURE RANGE panel

The DU-PROCEDURE ranges are used to enable DU failure simulations in your test.

- [DU-PROCEDURE range panel settings below](#)
- [DU Failure Parameters below](#)



DU-PROCEDURE range panel settings

When you select a DU-PROCEDURE range from the **DU-CP Range** panel, DuSIM opens the **DU-PROCEDURE** panel, from which you can:

- Select the **Delete** button to delete the selected DU-PROCEDURE range from the test configuration.
- Configure the settings for the selected DU-PROCEDURE range.

The following table describes the available settings that are required for each DU-PROCEDURE range.

Setting	Description
Name	You can accept or modify the default range name assigned by DuSIM.
DU Failure Scenario	Select to open the DU Failure Parameters below panel.

DU Failure Parameters

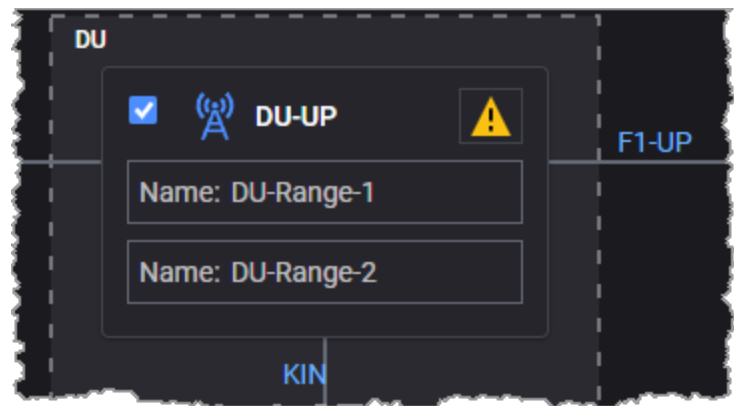
The following table describes the DU Failure Parameters.

Setting	Description
DU OffAir/OnAir Simulation Enabled	Enable this option to simulate a DU going off the air then back on.

Setting	Description
Loop Enabled	Enable this option to loop through the failure scenario. When not enabled, the simulated failure occurs one time only.
DU Failure Count	The number of DUs in the range that will simulate the failure.
DU Failure Trigger Time (s)	Set the number of seconds to elapse before the failure occurs.
DU Recovery Time (s)	Set the number of seconds that the DU will remain off, once the simulated failure has been triggered.

CHAPTER 9

DU-UP configuration settings



The gNB Distributed Unit (gNB-DU) is a logical node hosting RLC, MAC, and PHY layers of the gNB, and its operation is partly controlled by a gNB-CU. One gNB-DU supports one or multiple cells, and it terminates the F1 interface connected with the gNB-CU.

In the DuSIM test topology, the gNB-DU is logically structured as two entities:

- DU-CP, which connective with the CU over the F1-C interface, which carries control plane traffic.
- DU-UP, which connective with the CU over the F1-U interface, which carries user plane traffic.

The chapter describes the **DU-UP** settings.

Chapter contents:

DU-UP RANGES panel	89
DU-UP Range panel	90

DU-UP RANGES panel

The **DU-UP RANGES** panel opens when you select the DU-UP node from the network topology window. You can perform the following tasks from this panel:

- Open a DU-UP range configuration for editing or viewing.
- Enable or disable a range for the test configuration.

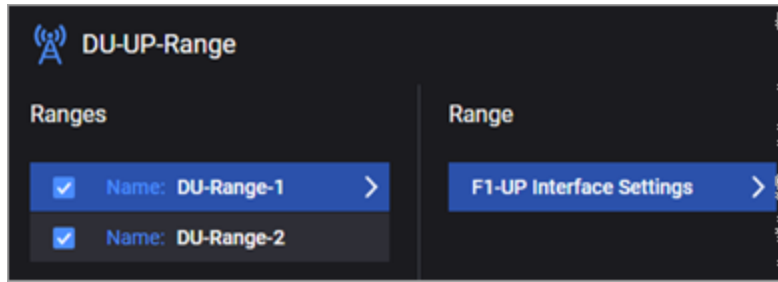
For example ...



DuSIM manages DU-UP ranges as follows:

- DuSIM automatically creates one DU-UP range for each DU-CP range that you configure in the test.
- If you delete a DU-CP range, DuSIM automatically deletes the corresponding DU-UP range.
- Although you cannot directly delete a DU-UP range, you can deselect a range for the test session. When you deselect a DU-UP range, DuSIM does not deselect the corresponding DU-CP range.

DU-UP Range panel



When you select a DU-UP range from the **DU-UP Ranges** panel, DuSIM opens the **Range** panel, from which you configure the F1-UP interface range settings. The DU-UP Range settings enable communication between the simulated DUs and your DUT.

They include the following groups of settings:

- [F1 Interface Settings below](#)
- [Connectivity Settings below](#)

F1 Interface Settings

The DU F1-UP interface settings specify the following set of configuration parameters.

Setting	Description
MTU	The desired Maximum Transmission Unit (MTU) for the F1 interface. The MTU specifies the largest packet that an Ethernet frame can carry.
T3 Response Timer	T3 timer value for GTP Echo Response messages, in seconds. This is the maximum amount of time to wait for a response from a request message.
N3 Requests	N3 counter value for Echo Request messages. This is the maximum number of retransmissions that will be permitted for a specific request message.
Echo Request Period	The time interval to use for sending periodic echo requests over the interface. This is the number of seconds to wait before sending the next Echo Request following receipt of the previous response.
Include Sequence Number	Select this option if you want DuSIM to include sequence numbers in T-PDUs.

Connectivity Settings

The F1-UP connectivity settings are organized into the following groups:

- [IP Settings on the next page](#)
- [MAC Settings on the next page](#)
- [VLAN settings on the next page](#)
- [IPsec settings on page 92](#)

IP Settings

These settings specify the properties of the F1-UP IP interface.

Setting	Description
IP	Enter the IP address for the first DU-UP node in this range. This is the user plane IP address for the simulated DUs. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the DU-UP nodes that are defined in this range will be incremented. The number of IP addresses that will be created is determined by the <i>Range Count</i> value configured for the <i>Parent DU-CP</i> .
IP Prefix Length	The subnet prefix length associated with this DU-UP IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
UDP Port	The UDP port number for this F1-UP IP interface.
UDP Checksum	The UDP checksum for this F1-UP IP interface.
Gateway Address	This DU-UP node's gateway address.

MAC Settings

These settings specify the properties of the F1-UP MAC interface.

Setting	Description
MAC	Specify the first media access control (MAC) address that will be assigned to the DU-UP node defined in this range. The default value is an auto-generated address that you can change, if desired.
MAC Increment	Specify the value (expressed as a 12-character alphanumeric MAC address value) by which the MAC addresses of all the DU-UP nodes that are defined in this range will be incremented.

VLAN settings

The following VLAN settings are available for the DU-UP F1 interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting.

Setting	Description
VLAN	Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

IPsec settings

The following IPsec settings are available for the DU-CP F1 interfaces.

Setting	Description
Destination Port	The IPsec tunnel's destination port.
Source Port	The IPsec tunnel's source port.
IP	The IP address of the F1-U interface on the DU range.
Role	<p>The role that this interface will play in the test:</p> <ul style="list-style-type: none"> • Initiator (Site-to-Site): The node will function as the initiator in the test (will initiate the tunnels). This option is used for site-to-site tests. • Initiator (Remote Access): The node will function as the initiator in the test (will initiate the tunnels). This option is used for Remote Access scenarios, in which an individual client is connected to a LAN through a secure tunnel. In this scenario, the client is operating as its own Secure Gateway. <p>The default value is <i>Initiator (Site-to-Site)</i>.</p>
<i>IPsec Authentication settings:</i>	
Authentication Method	<p>Select the authentication method to use in this configuration. The options are:</p> <ul style="list-style-type: none"> • Certificates: Use CA certificates for authentication. • Pre-Shared Key: Use a pre-shared key rather than certificates.
CA Certificate	Select a CA certificate that you have previously uploaded. Uploading certificates is managed in the DuSIM Global settings. Refer to CA Certificates Settings on page 57 for instructions.
Certificate and Private Keys	<p>To upload a zip file that contains the certificate file (extension .crt) and the private key (extension .key):</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Upload. <p>Note that the two files contained in the zip file should have the same file name (such as cert10.crt and cert10.key).</p> <p>To remove a zip file that has been previously uploaded:</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Clear.

Setting	Description
Use Same Certificate and Private Key for all Instances	Use the uploaded certificate and key file for all test instances of this configuration.
<i>IPsec IKE Phase 1 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
DH Group	<p>Specifies the Diffie-Hellman (DH) Group.</p> <p>The DH key exchange algorithm allows two parties to jointly establish a shared secret key over an insecure communications channel. DH groups determine the strength of the key used in the key exchange process. The higher the group number, the more secure the key. For example, DH group 1 is a 768-bit group and DH group 2 is a 1024-bit group.</p>
PRF Algorithm	<p>Specifies the algorithm used to perform Pseudo-Random Functions (key derivations).</p> <p>The PRF choices are...</p> <ul style="list-style-type: none"> • HMAC-MD5: Hash-based Message Authentication Code, Message-Digest Algorithm 5. • HMAC-SHA1: Hash-based Message Authentication Code, Secure Hash Algorithm 1. • HMAC-SHA256: Hash-based Message Authentication Code, Secure Hash Algorithm 256. • HMAC-SHA384: Hash-based Message Authentication Code, Secure Hash Algorithm 384. • HMAC-SHA512: Hash-based Message Authentication Code, Secure Hash Algorithm 512.

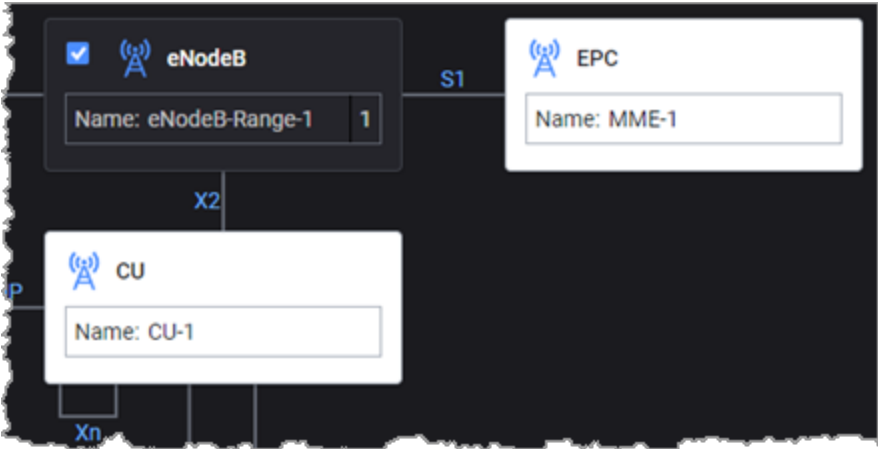
Setting	Description
<i>IPsec IKE Phase 2 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
<i>IPsec Identification settings:</i>	
Local Identification Type	<p>The Identification Type field describes the type of information contained in the IPsec packet Identification Data field. See RFC 2407 for more information.</p> <p>The choices are...</p> <ul style="list-style-type: none"> • ID_IP_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as a single four-octet IPv4 address. • ID_FQDN: Sets the Identification Type field to 2 and inserts the gateway address into the Identification Data field as a fully-qualified domain name string. For example, "foo.bar.com". • ID_USER_FQDN: Sets the Identification Type field to 3 and inserts the gateway address into the Identification Data field as a fully-qualified username string. For example, "piper@foo.bar.com". • ID_Iv6P_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as an IPv6 address. • ID_DER_ASN1_DN: Sets the Identification Type field to 9 and inserts the gateway address into the Identification Data field as a binary DER encoding of an ASN.1 X.500 Certificate Distinguished Name. • ID_KEY_ID: Sets the Identification Type field to 11 and inserts the gateway address into the Identification Data field as an opaque byte stream that may be used to pass vendor-specific information necessary to identify which pre-shared key should be used to authenticate Aggressive mode negotiations. ID_KEY_ID is recommended for Network Access Identifiers (NAIs) that do not

Setting	Description
	include the realm component (reference: draft-eronen-ipsec-ikev2-clarifications). ID_KEY_ID is supported by IKEv2 only.
Local Identification Value	The Local Identification Value is a string value, with a maximum of 1024 characters.
<i>IPsec Timers settings:</i>	
Enable Rekey	Enables or disables renegotiation of Phase 1 and Phase 2 SAs on expiry of tunnel lifetimes: <ul style="list-style-type: none"> • When disabled, tunnels are torn down when their lifetimes expire. • When enabled, the tunnels' Phase 1 and Phase 2 options are renegotiated before their lifetimes expire, and the tunnels stay up.
IKE Phase 1 (IKE) Lifetime	Specifies the Phase 1 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.
IKE Phase 2 (ESP) Lifetime	Specifies the Phase 2 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.
DPD Interval	<p>When this value is set to a value greater than zero, each IKE peer in the range uses the Dead Peer Detection (DPD) protocol to determine proof of liveness of the other peer. The peers send DPD HELLO messages according to the interval that you specify.</p> <p>When the value is set to zero, the IKE peers do not send DPD HELLO messages.</p> <p>An IPsec endpoint uses DPD to confirm that its peer is still up. DPD is implemented in IKE through the use of an asynchronous, bidirectional message exchange:</p> <ul style="list-style-type: none"> • DPD HELLO • DPD HELLO ACK <p>A complete DPD exchange (transmission of DPD HELLO and receipt of the corresponding DPD HELLO ACK) serves as proof of liveness. If a node does not receive a response to a DPD HELLO within a specified time, it assumes that the peer is dead or unreachable, and tears down the tunnel.</p>

CHAPTER 10

eNodeB configuration settings

The eNodeB node acts as the master eNodeB (MeNB) for the NSA network topology. One eNodeB supports one or multiple LTE cells, and it terminates the S1 interface connected with the LTE Core network (EPC) and the X2 interface connected with the gNB CU.



This chapter describes the eNodeB settings.

Chapter contents:

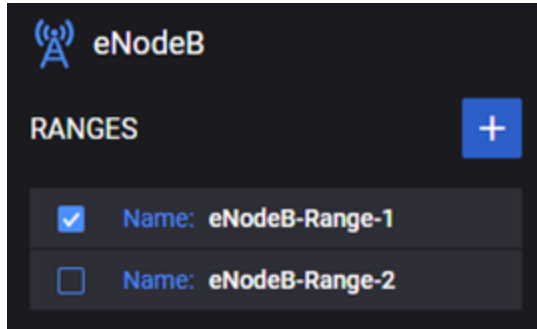
eNodeB RANGES panel	97
eNodeB RANGE panel	98
Cells settings	99
X2-C Interface Settings	100
X2-U Interface Settings	105
S1-C Interface Settings	107
S1-U Interface Settings	112

eNodeB RANGES panel

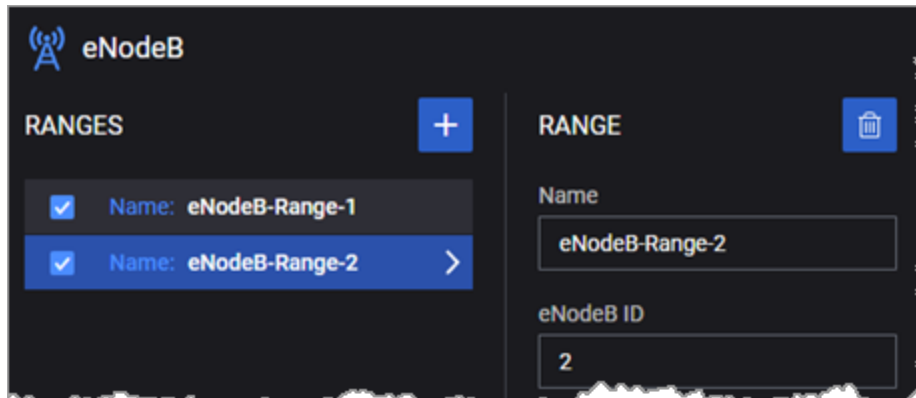
The eNodeB RANGES panel opens when you select the eNodeB node from the network topology window. You can perform the following tasks from this panel:

- Add a new eNodeB range to your test configuration.
- Open a eNodeB range configuration for editing or viewing.
- Enable or disable a range for the test configuration.

For example:



eNodeB RANGE panel



When you select an eNodeB range from the eNodeB RANGES panel, DuSIM opens the RANGE panel, from which you can:

- Select the Delete button to delete the selected eNodeB range from the test configuration.
- Configure the settings for the selected eNodeB range.

The following table describes the available settings that are required for each eNodeB range.

Setting	Description
Name	The simulated eNodeB Range Name. The default name is auto-generated and can be modified.
eNodeB ID	The eNodeB ID, specified as a decimal value.
Range Count	By default, a eNodeB range contains one eNodeB node. If you want to create multiple eNodeB nodes for the range, enter the desired number in this field.
Associated MME	Select the MME range to which this eNodeB range is linked over the S1 interface. The available values correspond to the MME Name parameter values configured for the EPC Node.
Associated gNodeB	Select the gNB-CU range to which this eNodeB is linked over the X2 interface.
Global ID Type	Select the Global ID type: Macro eNodeB ID or Home eNodeB ID.
Home MCC	The PLMN's mobile country code (MCC).
Home MNC	The PLMN's mobile network code (MNC).
Tracking Area Code	The unique identifier of the Tracking Area Code (TAC) to which this eNodeB belongs.

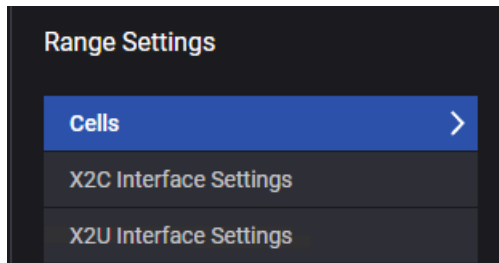
Range Settings:

The following sections describe the eNodeB cell settings and the various interface settings.

Cells settings	99
X2-C Interface Settings	100
X2-U Interface Settings	105
S1-C Interface Settings	107
S1-U Interface Settings	112

Cells settings

Each eNodeB range requires configuration of a group of Range Settings, which include the range's Cells settings.



Cells

Each eNodeB range requires configuration of a group of Cells settings, which are the LTE cells that this eNodeB range is simulating.

The following table describes the available settings that are required for Cells range:

Setting	Description
Cell ID	This parameter specifies the identifier of the physical cell (PCI) of LTE cells for this eNodeB range.
Cell ID Increment	Enter the value by which DuSIM will increment each Cell ID if the Cell Count is greater than 1.
Cell Count	Each eNodeB can have multiple cells. If you want to create multiple cells for the eNodeB range, enter the desired number in this field.
Mode	This parameter specifies the LTE technology. It is possible to choose one of the following values from the drop-down list: FDD, TDD.
UL-EARFCN	This parameter specifies the uplink EARFCN of the cell.
DL-EARFCN	This parameter specifies the downlink EARFCN of the cell.
Bandwidth UL	This parameter specifies the uplink frequency bandwidth of the cell in Mhz. It is

Setting	Description
	possible to change the setting by choosing a value from the drop-down list.
Bandwidth DL	This parameter specifies the downlink frequency bandwidth of the cell in Mhz. It is possible to change the setting by choosing a value from the drop-down list.
Subframe Assignment	This parameter specifies the Subframe Assignment in decimal format; it is meaningful only if the Mode parameter is set to TDD. Valid values are included in the range of 0 to 6. Refer to 3GPP TS 36.423, subclause 9.2.8 for details.
Special Subframe Pattern	This parameter specifies the Special Subframe Pattern in decimal format; it is meaningful only if the Mode parameter is set to TDD. Valid values are included in the range of 0 to 8. Refer to 3GPP TS 36.423, subclause 9.2.8 for details.
Cyclic Prefix UL	This parameter specifies the type of cyclic prefix to be applied in uplink. It is possible to choose one of the following values from the drop-down list: Normal, Extended.
Cyclic Prefix DL	This parameter specifies the type of cyclic prefix to be applied in downlink. It is possible to choose one of the following values from the drop-down list: Normal, Extended.
Frequency band Indicator	This parameter specifies the Frequency Band Indicator in decimal format. Valid values are included in the range of 1 to 256. Refer to 3GPP TS 36.423 for details.

X2-C Interface Settings

The X2-C interface settings specify the properties and connectivity information of the X2 control plane interface connected with gNB-CU.

Interface Settings

The following table describes the available settings that are required:

Setting	Description
MTU	The desired Maximum Transmission Unit (MTU) for the X2 Control Plane interface. The MTU specifies the largest packet that an Ethernet frame can carry.
Initiated ENDC X2 Setup	This checkbox enables/disables initiating an SCTP association on the X2 interface.

Connectivity Settings

The X2C connectivity settings are organized into the following groups:

- [IP Settings on the next page](#)
- [VLAN Settings on the next page](#)

- [IPsec Settings below](#)

IP Settings

These settings specify the properties of the eNodeB X2-C IP interface.

Setting	Description
IP Address	Enter the IP address for X2AP interface that the first DuSIM eNodeB node defined in this range will use to communicate with the gNB-CU (device under test).
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the eNodeB nodes that are defined in this range will be incremented. The number of IP addresses that will be created is determined by the Range Count RANGE value.
IP Prefix Length	The subnet prefix length associated with X2AP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Port	The port number on which the node listens on the X2-C interface. The port can be in the range from 1 through 65535.
Gateway Address	This eNodeB node's gateway address towards X2AP interface of gNB-CU.

VLAN Settings

The following VLAN settings are available for the eNodeB X2-C interface.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

IPsec Settings

The following IPsec settings are available for the eNodeB X2-C interface.

Setting	Description
Destination Port	The IPsec tunnel's destination port.
Source Port	The IPsec tunnel's source port.
IP	The IP address of the S1C interface on the eNodeB range.
Role	The role that this interface will play in the test: <ul style="list-style-type: none"> • Initiator (Site-to-Site): The node will function as the initiator in the test (will initiate the tunnels). This option is used for site-to-site tests.

Setting	Description
	<ul style="list-style-type: none"> • Initiator (Remote Access): The node will function as the initiator in the test (will initiate the tunnels). This option is used for Remote Access scenarios, in which an individual client is connected to a LAN through a secure tunnel. In this scenario, the client is operating as its own Secure Gateway. <p>The default value is <i>Initiator (Site-to-Site)</i>.</p>
<i>IPsec Authentication settings:</i>	
Authentication Method	<p>Select the authentication method to use in this configuration. The options are:</p> <ul style="list-style-type: none"> • Certificates: Use CA certificates for authentication. • Pre-Shared Key: Use a pre-shared key rather than certificates.
CA Certificate	<p>Select a CA certificate that you have previously uploaded. Uploading certificates is managed in the DuSIM Global settings. Refer to CA Certificates Settings on page 57 for instructions.</p>
Certificate and Private Keys	<p>To upload a zip file that contains the certificate file (extension .crt) and the private key (extension .key):</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Upload. <p>Note that the two files contained in the zip file should have the same file name (such as cert10.crt and cert10.key).</p> <p>To remove a zip file that has been previously uploaded:</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Clear.
Use Same Certificate and Private Key for all Instances	<p>Use the uploaded certificate and key file for all test instances of this configuration.</p>
<i>IPsec IKE Phase 1 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16

Setting	Description
	<p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
DH Group	<p>Specifies the Diffie-Hellman (DH) Group.</p> <p>The DH key exchange algorithm allows two parties to jointly establish a shared secret key over an insecure communications channel. DH groups determine the strength of the key used in the key exchange process. The higher the group number, the more secure the key. For example, DH group 1 is a 768-bit group and DH group 2 is a 1024-bit group.</p>
PRF Algorithm	<p>Specifies the algorithm used to perform Pseudo-Random Functions (key derivations).</p> <p>The PRF choices are...</p> <ul style="list-style-type: none"> • HMAC-MD5: Hash-based Message Authentication Code, Message-Digest Algorithm 5. • HMAC-SHA1: Hash-based Message Authentication Code, Secure Hash Algorithm 1. • HMAC-SHA256: Hash-based Message Authentication Code, Secure Hash Algorithm 256. • HMAC-SHA384: Hash-based Message Authentication Code, Secure Hash Algorithm 384. • HMAC-SHA512: Hash-based Message Authentication Code, Secure Hash Algorithm 512.
<i>IPsec IKE Phase 2 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>

Setting	Description
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
<i>IPsec Identification settings:</i>	
Local Identification Type	<p>The Identification Type field describes the type of information contained in the IPsec packet Identification Data field. See RFC 2407 for more information.</p> <p>The choices are...</p> <ul style="list-style-type: none"> • ID_IP_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as a single four-octet IPv4 address. • ID_FQDN: Sets the Identification Type field to 2 and inserts the gateway address into the Identification Data field as a fully-qualified domain name string. For example, "foo.bar.com". • ID_USER_FQDN: Sets the Identification Type field to 3 and inserts the gateway address into the Identification Data field as a fully-qualified username string. For example, "piper@foo.bar.com". • ID_Iv6P_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as an IPv6 address. • ID_DER_ASN1_DN: Sets the Identification Type field to 9 and inserts the gateway address into the Identification Data field as a binary DER encoding of an ASN.1 X.500 Certificate Distinguished Name. • ID_KEY_ID: Sets the Identification Type field to 11 and inserts the gateway address into the Identification Data field as an opaque byte stream that may be used to pass vendor-specific information necessary to identify which pre-shared key should be used to authenticate Aggressive mode negotiations. ID_KEY_ID is recommended for Network Access Identifiers (NAIs) that do not include the realm component (reference: draft-eronen-ipsec-ikev2-clarifications). ID_KEY_ID is supported by IKEv2 only.
Local Identification Value	The Local Identification Value is a string value, with a maximum of 1024 characters.
<i>IPsec Timers settings:</i>	
Enable Rekey	<p>Enables or disables renegotiation of Phase 1 and Phase 2 SAs on expiry of tunnel lifetimes:</p> <ul style="list-style-type: none"> • When disabled, tunnels are torn down when their lifetimes expire. • When enabled, the tunnels' Phase 1 and Phase 2 options are renegotiated before their lifetimes expire, and the tunnels stay up.
IKE Phase 1 (IKE) Lifetime	<p>Specifies the Phase 1 Security Association (SA) lifetime, in seconds.</p> <p>The valid range of values is 0 through 31,557,600.</p>

Setting	Description
IKE Phase 2 (ESP) Lifetime	Specifies the Phase 2 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.
DPD Interval	<p>When this value is set to a value greater than zero, each IKE peer in the range uses the Dead Peer Detection (DPD) protocol to determine proof of liveness of the other peer. The peers send DPD HELLO messages according to the interval that you specify.</p> <p>When the value is set to zero, the IKE peers do not send DPD HELLO messages.</p> <p>An IPsec endpoint uses DPD to confirm that its peer is still up. DPD is implemented in IKE through the use of an asynchronous, bidirectional message exchange:</p> <ul style="list-style-type: none"> • DPD HELLO • DPD HELLO ACK <p>A complete DPD exchange (transmission of DPD HELLO and receipt of the corresponding DPD HELLO ACK) serves as proof of liveness. If a node does not receive a response to a DPD HELLO within a specified time, it assumes that the peer is dead or unreachable, and tears down the tunnel.</p>

X2-U Interface Settings

The X2-U interface settings specify the properties and connectivity information of X2 user plane interface connected with gNB-CU. The following table describes the available settings that are required:

Setting	Description
MTU	The desired Maximum Transmission Unit (MTU) for the F1 interface. The MTU specifies the largest packet that an Ethernet frame can carry.
T3 Response Timer	T3 timer value for GTP Echo Response messages, in seconds. This is the maximum amount of time to wait for a response from a request message.
N3 Requests	N3 counter value for Echo Request messages. This is the maximum number of retransmissions that will be permitted for a specific request message.
Echo Request Period	The time interval to use for sending periodic echo requests over the interface. This is the number of seconds to wait before sending the next Echo Request following receipt of the previous response.
Include Sequence Number	Select this option if you want DuSIM to include sequence numbers in T-PDUs.

Connectivity Settings

The connectivity settings include the IP address values plus the layer 2 values for the user plane traffic.

Setting	Description
<i>IP settings:</i>	
IP Address	Enter the IP address for the first eNodeB node in this range. This is the user plane IP address for the simulated eNodeBs for X2 interface. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the eNodeB nodes that are defined in this range will be incremented. The number of IP addresses that will be created is determined by the Range Count value configured for the Parent eNodeB.
IP Prefix Length	The subnet prefix length associated with this eNodeB X2 user plane IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
UDP Port	The UDP port number that will be used for this interface in this range. The default port is 2152 (a registered GTP user plane port).
UDP Checksum	Enable this option if you want DuSIM to perform checksum computation for this range.
Gateway Address	This eNodeB node's gateway address towards X2AP interface of gNB-CU.
<i>MAC settings:</i>	
MAC	Specify the first media access control (MAC) address that will be assigned to the eNodeB X2 interface defined in this range. The default value is an auto-generated address that you can change, if desired.
MAC Increment	Specify the value (expressed as a 12-character alphanumeric MAC address value) by which the MAC addresses of all the eNodeB X2 interface defined in this range will be incremented.
<i>VLAN settings:</i>	
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID.
Inner VLAN	When Outer VLAN is enabled, DuSIM exposes the optional Inner VLAN setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID.

S1-C Interface Settings

The S1-C interface settings specify the properties and connectivity information of S1 control plane interface connected with the EPC.

S1-C Interface Settings

The S1-C interface settings specify the following configuration parameters.

Setting	Description
MTU	The desired Maximum Transmission Unit (MTU) for the S1-C interface. The MTU specifies the largest packet that an Ethernet frame can carry.

S1-C Connectivity Settings

The S1-C connectivity settings are organized into the following groups:

- [IP Settings below](#)
- [VLAN settings on the facing page](#)
- [IPsec settings on the facing page](#)

IP Settings

These settings specify the properties of the F1-UP IP interface.

Setting	Description
IP	Enter the IP address for the first eNodeB node in this range. This is the user plane IP address for the simulated eNodeBs for X2 interface. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the eNodeB nodes that are defined in this range will be incremented. The number of IP addresses that will be created is determined by the Range Count value configured for the Parent eNodeB.
IP Prefix Length	The subnet prefix length associated with this eNodeB X2 user plane IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Port	The S1AP port number to use. The default is 36412.
Gateway Address	This eNodeB node's gateway address towards the S1AP interface of EPC.

VLAN settings

The following VLAN settings are available for the eNodeB S1C interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

IPsec settings

The following IPsec settings are available for the eNodeB S1C interfaces.

Setting	Description
Destination Port	The IPsec tunnel's destination port.
Source Port	The IPsec tunnel's source port.
IP	The IP address of the S1C interface on the eNodeB range.
Role	<p>The role that this interface will play in the test:</p> <ul style="list-style-type: none"> • Initiator (Site-to-Site): The node will function as the initiator in the test (will initiate the tunnels). This option is used for site-to-site tests. • Initiator (Remote Access): The node will function as the initiator in the test (will initiate the tunnels). This option is used for Remote Access scenarios, in which an individual client is connected to a LAN through a secure tunnel. In this scenario, the client is operating as its own Secure Gateway. <p>The default value is <i>Initiator (Site-to-Site)</i>.</p>
<i>IPsec Authentication settings:</i>	
Authentication Method	<p>Select the authentication method to use in this configuration. The options are:</p> <ul style="list-style-type: none"> • Certificates: Use CA certificates for authentication. • Pre-Shared Key: Use a pre-shared key rather than certificates.
CA Certificate	Select a CA certificate that you have previously uploaded. Uploading certificates is managed in the DuSIM Global settings. Refer to CA Certificates Settings on page 57 for instructions.
Certificate and Private Keys	<p>To upload a zip file that contains the certificate file (extension .crt) and the private key (extension .key):</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Upload.

Setting	Description
	<p>Note that the two files contained in the zip file should have the same file name (such as cert10.crt and cert10.key).</p> <p>To remove a zip file that has been previously uploaded:</p> <ol style="list-style-type: none"> 1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file. 2. Click Clear.
Use Same Certificate and Private Key for all Instances	Use the uploaded certificate and key file for all test instances of this configuration.
<i>IPsec IKE Phase 1 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
DH Group	<p>Specifies the Diffie-Hellman (DH) Group.</p> <p>The DH key exchange algorithm allows two parties to jointly establish a shared secret key over an insecure communications channel. DH groups determine the strength of the key used in the key exchange process. The higher the group number, the more secure the key. For example, DH group 1 is a 768-bit group and DH group 2 is a 1024-bit group.</p>
PRF Algorithm	<p>Specifies the algorithm used to perform Pseudo-Random Functions (key derivations).</p> <p>The PRF choices are...</p> <ul style="list-style-type: none"> • HMAC-MD5: Hash-based Message Authentication Code, Message-Digest Algorithm 5. • HMAC-SHA1: Hash-based Message Authentication Code, Secure Hash Algorithm 1.

Setting	Description
	<ul style="list-style-type: none"> • HMAC-SHA256: Hash-based Message Authentication Code, Secure Hash Algorithm 256. • HMAC-SHA384: Hash-based Message Authentication Code, Secure Hash Algorithm 384. • HMAC-SHA512: Hash-based Message Authentication Code, Secure Hash Algorithm 512.
<i>IPsec IKE Phase 2 settings:</i>	
Encryption Algorithm	<p>Specifies the encryption algorithm used to protect communications during message exchanges.</p> <p>Available algorithms ...</p> <ul style="list-style-type: none"> • AES128-CBC • AES192-CBC • AES256-CBC • AES128-GCM-16 • AES192-GCM-16 • AES256-GCM-16 <p>Note that the -GCM algorithms are AEAD (Authenticated Encryption with Associated Data) algorithms: they also provide hashing.</p> <p>Refer to RFC-4106 for details about the use of AES and GCM as an IPsec ESP mechanism.</p>
Hash Algorithm	The hash algorithm to use for IPsec message exchanges.
<i>IPsec Identification settings:</i>	
Local Identification Type	<p>The Identification Type field describes the type of information contained in the IPsec packet Identification Data field. See RFC 2407 for more information.</p> <p>The choices are...</p> <ul style="list-style-type: none"> • ID_IP_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as a single four-octet IPv4 address. • ID_FQDN: Sets the Identification Type field to 2 and inserts the gateway address into the Identification Data field as a fully-qualified domain name string. For example, "foo.bar.com". • ID_USER_FQDN: Sets the Identification Type field to 3 and inserts the gateway address into the Identification Data field as a fully-qualified username string. For example, "piper@foo.bar.com". • ID_Iv6P_ADDR: Sets the Identification Type field to 1 and inserts the gateway address into the Identification Data field as an IPv6 address. • ID_DER_ASN1_DN: Sets the Identification Type field to 9 and inserts the gateway address into the Identification Data field as a binary DER

Setting	Description
	<p>encoding of an ASN.1 X.500 Certificate Distinguished Name.</p> <ul style="list-style-type: none"> • ID_KEY_ID: Sets the Identification Type field to 11 and inserts the gateway address into the Identification Data field as an opaque byte stream that may be used to pass vendor-specific information necessary to identify which pre-shared key should be used to authenticate Aggressive mode negotiations. ID_KEY_ID is recommended for Network Access Identifiers (NAIs) that do not include the realm component (reference: draft-eronen-ipsec-ikev2-clarifications). ID_KEY_ID is supported by IKEv2 only.
Local Identification Value	The Local Identification Value is a string value, with a maximum of 1024 characters.
<i>IPsec Timers settings:</i>	
Enable Rekey	<p>Enables or disables renegotiation of Phase 1 and Phase 2 SAs on expiry of tunnel lifetimes:</p> <ul style="list-style-type: none"> • When disabled, tunnels are torn down when their lifetimes expire. • When enabled, the tunnels' Phase 1 and Phase 2 options are renegotiated before their lifetimes expire, and the tunnels stay up.
IKE Phase 1 (IKE) Lifetime	<p>Specifies the Phase 1 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.</p>
IKE Phase 2 (ESP) Lifetime	<p>Specifies the Phase 2 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.</p>
DPD Interval	<p>When this value is set to a value greater than zero, each IKE peer in the range uses the Dead Peer Detection (DPD) protocol to determine proof of liveness of the other peer. The peers send DPD HELLO messages according to the interval that you specify.</p> <p>When the value is set to zero, the IKE peers do not send DPD HELLO messages. An IPsec endpoint uses DPD to confirm that its peer is still up. DPD is implemented in IKE through the use of an asynchronous, bidirectional message exchange:</p> <ul style="list-style-type: none"> • DPD HELLO • DPD HELLO ACK <p>A complete DPD exchange (transmission of DPD HELLO and receipt of the corresponding DPD HELLO ACK) serves as proof of liveness. If a node does not receive a response to a DPD HELLO within a specified time, it assumes that the peer is dead or unreachable, and tears down the tunnel.</p>

S1-U Interface Settings

The S1-U interface settings specify the properties and connectivity information of S1 user plane interface connected with EPC. The following table describes the available settings that are required:

Setting	Description
MTU	The desired Maximum Transmission Unit (MTU) for the F1 interface. The MTU specifies the largest packet that an Ethernet frame can carry.
T3 Response Timer	T3 timer value for GTP Echo Response messages, in seconds. This is the maximum amount of time to wait for a response from a request message
N3 Requests	N3 counter value for Echo Request messages. This is the maximum number of retransmissions that will be permitted for a specific request message.
Echo Request Period	The time interval to use for sending periodic echo requests over the interface. This is the number of seconds to wait before sending the next Echo Request following receipt of the previous response.
Include Sequence Number	Select this option is you want DuSIM to include sequence numbers in T-PDUs for this interface range.

Connectivity Settings

The connectivity settings include the IP address values plus the layer 2 values for the user plane traffic.

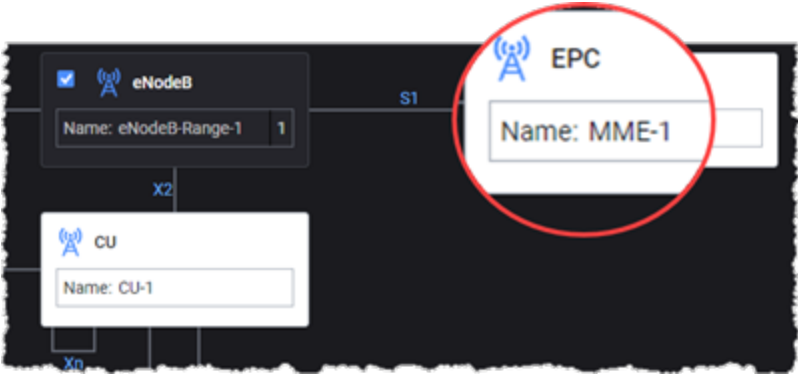
Setting	Description
<i>IP settings:</i>	
IP Address	Enter the IP address for the first eNodeB node in this range. This is the user plane IP address for the simulated eNodeB for S1 interface. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the eNodeB nodes that are defined in this range will be incremented. The number of IP addresses that will be created is determined by the Range Count value configured for the Parent eNodeB.
IP Prefix Length	The subnet prefix length associated with this eNodeB X2 user plane IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
UDP Port	The UDP port number that will be used for this interface in this range. The default port is 2152 (a registered GTP user plane port).
UDP Checksum	Enable this option if you want DuSIM to perform checksum computation for this range.

Setting	Description
Gateway Address	This eNodeB node's gateway address towards S1 interface of the EPC.
<i>Gateway Address</i>	
MAC settings:	Specify the first media access control (MAC) address that will be assigned to the eNodeB X2 interface defined in this range. The default value is an auto-generated address that you can change, if desired.
MAC Increment	Specify the value (expressed as a 12-character alphanumeric MAC address value) by which the MAC addresses of this interface will be incremented.
<i>VLAN settings:</i>	
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID.
Inner VLAN	When Outer VLAN is enabled, DuSIM exposes the optional Inner VLAN setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID.

CHAPTER 11

EPC configuration settings

EPC (Evolved Packet Core) is the 4G core network for NSA topology. The EPC is an external entity and can be the device under test (DUT) in a Keysight DuSIM test configuration or simulated by Keysight CoreSIM product.



Chapter contents:

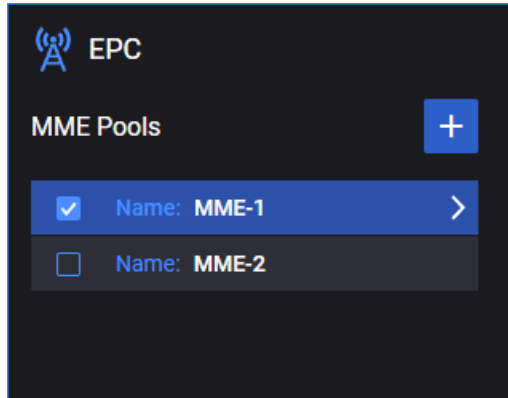
MME Pools panel	115
MME panel	116

MME Pools panel

The MME Pools panel opens when you select the EPC node from the network topology window. You can perform the following tasks from this panel:

- Add a new MME to your test configuration.
- Open a MME configuration for editing or viewing.
- Enable or disable a MME for the test session.

For example:



MME panel

When you select a node from the MME Pools panel, DuSIM opens the MME panel, from which you can:

- Delete the selected MME from the test configuration.
- Modify the MME name.
- Modify the MME Group ID value
- Select Connectivity Settings to configure the IP and (optionally) IPsec configuration settings for the MME.

The following Connectivity Settings are available:

- [IP Settings below](#)
- [IPsec Settings below](#)

IP Settings

These settings specify the properties of the MME IP interface.

Setting	Description
IP Address	Enter the IP address for this MME node.
IP Prefix Length	The subnet prefix length associated with this MME IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

IPsec Settings

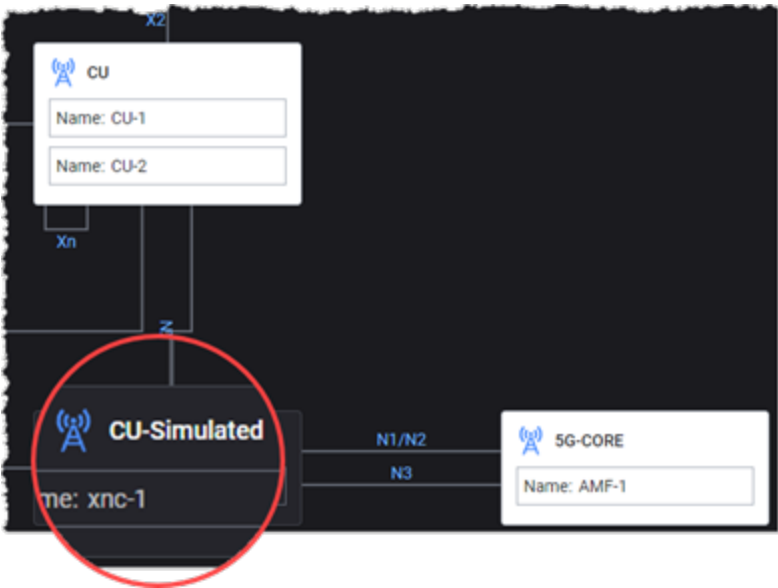
The following table describes the MME IPsec settings. To enable IPsec on this interface, the MME needs only the IP address, prefix, and port number of the client-side IPsec tunnel. Refer to [S1-C Interface Settings on page 107](#) for the client-side IPsec configuration settings.

Setting	Description
Source Port	The IPsec tunnel's source port.
IP Address	The IP address of the F1-C interface on the eNodeB range.
IP Prefix Length	The IP address subnet prefix length associated with this IPsec interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

CHAPTER 12

CU-Simulated configuration settings

The CU-Simulated node acts as simulated endpoint of the Xn interface connection with gNB-CU node (the DUT) in a DuSIM test configuration.



The CU-Simulated node also establishes connectivity over the N2/N3 interfaces with the 5G Core network.

Chapter contents:

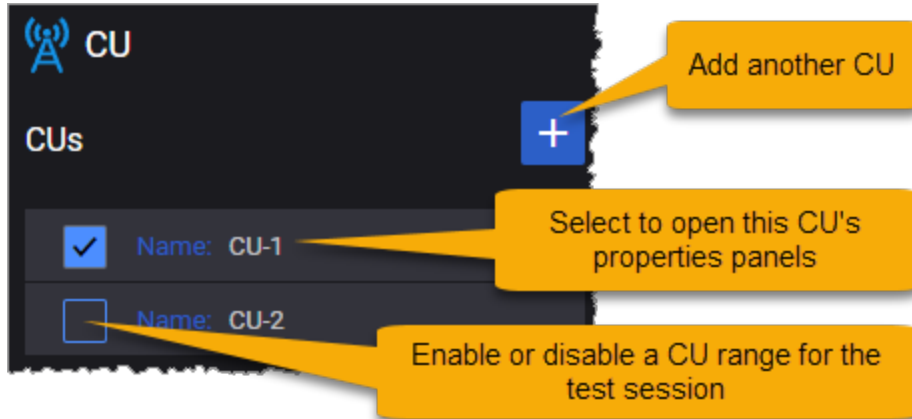
CU-Simulated Ranges panel	119
CU-Simulated Range panel	120
Node Settings	120
Cells Settings	121
Subscriber Settings	122
N2 Interface Settings	124
N3 Interface Settings	126
Xn-C Interface Settings	127
Xn-U Interface Settings	128

CU-Simulated Ranges panel

The CU-Simulated RANGES panel opens when you select the CU-Simulated node from the network topology window. You can perform the following tasks from this panel:

- Add a new CU-Simulated range to your test configuration.
- Open a CU-Simulated range configuration for editing or viewing.
- Enable or disable a range for the test configuration.

For example:



CU-Simulated Range panel

When you select a CU-Simulated range from the CU-Simulated RANGES panel, DuSIM opens the RANGE panel, from which you can:

- Select the Delete button to delete the selected CU-Simulated range from the test configuration.
- Configure the node, cell, subscriber, and interface settings for the selected CU-Simulated range.

The following sections describe the available settings that are required for each CU-Simulated range:

Node Settings	120
Cells Settings	121
Subscriber Settings	122
N2 Interface Settings	124
N3 Interface Settings	126
Xn-C Interface Settings	127
Xn-U Interface Settings	128

Node Settings

Each CU-Simulated range requires configuration of node settings. The following table describes the available node settings that are required for each range:

Setting	Description
Name	Each Simulated CU node instance is identified by a Name. You can accept the value provided by DuSIM or overwrite it with your own value.
Associated CU	This parameter specifies the name of the linked DUT gNB-CU. Available CU node names are provided for selection.
PLMN MCC	The PLMN MCC for this Simulated CU range.
PLMN MNC	The PLMN MNC for this Simulated CU range.
Tracking Area Code	The Tracking Area Code to use for the nodes in this range.
Region ID	The AMF Region ID to use. This ID identifies the region in which the node resides. The AMF Region ID addresses the case that there are more AMFs in the network than the number of AMFs that can be supported by AMF Set ID and AMF Pointer. It allows operators to re-use the same AMF Set IDs and AMF Pointers in different regions.
Set ID	The AMF Set ID to use. The Set ID uniquely identifies the AMF Set within the AMF Region.

Setting	Description
Pointer	The AMF Pointer identifies one or more AMFs within the AMF Set.
CU ID	The Simulated gNB CU Identifier.
CU ID length	The number of bits (from the NRCGI) to use for the CU ID. (The number of bits to use for the DU ID is a vendor decision.) It can be configured to use between 22 bits and 32 bits.
CU ID Count	Number of CU IDs to use
CU ID Increment	Increment step for CU ID.
Connection Timeout	Connection timeout in milliseconds (ms) for this node.


Cells Settings


Each CU-Simulated range requires configuration of a group of Cells settings, which are the simulated cells for this node. The following table describes the available Cells settings that are required for each range:

Setting	Description
Cell ID	The NR Cell Global Identifier (NRCGI)
Cell ID Increment	Enter the value by which DuSIM will increment each Cell ID if the Cell Count is greater than 1.
Cell Count	Each simulated CU can have multiple cells. If you want to create multiple cells for the CU-Simulated range, enter the desired number in this field.
PLMN Identity	<p>The Public Land Mobile Network (PLMN) in which this cell is located.</p> <p>The PLMN is a globally unique identifier that comprises the MCC and MNC:</p> <ul style="list-style-type: none"> • PLMN MCC: The PLMN's mobile country code (MCC). • PLMN MNC: The PLMN's mobile network code (MNC).

NSSAI

Each CU-Simulated range requires configuration of a group of NSSAI settings, which are described in the following table:

Setting	Description
	<p>The following actions are available:</p> <ul style="list-style-type: none"> • Select the Add NSSAI button to add a new NSSAI to your test configuration. • Select NSSAI from the list to access the configuration settings.

Setting	Description
<i>NSSAI panel:</i>	
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.
SST	The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the S-NSSAI information element. The standardized SST values are: <ul style="list-style-type: none"> • (eMBB) • (URLCC) • (MIoT)
SD	The Slice Differentiator (SD) value for this NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The Mapped configured Slice/Service Type (SST) value for this NSSAI.
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this NSSAI.

Subscriber Settings

Each CU-Simulated range requires configuration of a group of Subscriber settings.

Allowed SSC Modes

Select the Session and Service Continuity (SSC) Mode for the PDU Sessions that UEs in this range will initiate.

The 5G System supports multiple session and service continuity (SSC) modes to support the continuity requirements of various applications and services for the UE. The SSC mode associated with a PDU Session does not change during the lifetime of that Session. The following modes are specified in TS 23.501, section 5.6.9:

- **SSC Mode 1:** The network preserves the connectivity service provided to the UE. For PDU Sessions of type IPv4, IPv6, or IPv4v6, the IP address is preserved.
- **SSC Mode 2:** The network may release the connectivity service delivered to the UE and release the corresponding PDU Session. For PDU Sessions of type IPv4, IPv6, or IPv4v6, the network may release IP addresses that had been allocated to the UE.
- **SSC Mode 3:** Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated to allow for better service continuity. For PDU Sessions of type IPv4, IPv6, or IPv4v6, the IP address is not preserved in this mode when the PDU Session Anchor changes.



The value you select will be used as the route selection descriptor component value field in the UE Route Selection Policy (URSP). Refer to TS 23.501 and TS 24.526 for detailed information.

DRBs

You use the DRBs Config panel to configure one or more Data Radio Bearers (DRBs) for this Subscriber Range.

From the panel, you can select a DRB Config for editing and also add additional DRB configurations. Select the **Add DRBs Config** button to add a new DRB configuration:

To configure DRBs for a subscriber range, open the **DRBs** panel, from which you can add, delete, and select DRBs for the selected range of subscribers.

Setting	Description
<i>DRBs:</i>	
	Select the Add DRB button to add a new DRB for the selected subscriber range.
	Select the Delete DRB button to remove this DRB from the selected subscriber range configuration.
ID	The DRB ID.
RLC Mode	RLC Mode identifies the NR RLC Mode. <ul style="list-style-type: none"> • TM (Transparent Mode): No RLC Header, Buffering at Tx Only, No Segmentation/Reassembly, No feedback • UM (Un-Acknowledged Mode): RLC Header, Buffering at both Tx and Rx, Segmentation/Reassembly, No feedback • AM (Acknowledged Mode): RLC Header, Buffering at both Tx and Rx, Segmentation/Reassembly, Feedback (ACK/NACK)
<i>PDCP (Packet Data Convergence Protocol):</i>	
Uplink Sequence Number Size	The value of the PDCP sequence number for uplink. The length of a PDCP sequence number is either 12 or 18 bits.
Downlink Sequence Number Size	The value of the PDCP sequence number for downlink. The length of a PDCP sequence number is either 12 or 18 bits.
<i>SDAP (Service Data Adaptation Protocol):</i>	
SDAP Uplink Header	Enable this option if an SDAP header should be included for this DRB for Uplink Data. SDAP is responsible for mapping between a quality-of-service flow (QoS Flow) from the 5GCore network and data radio bearer (DRB).
SDAP Downlink Header	Enable this option if an SDAP header should be included for this DRB for Downlink Data.

N2 Interface Settings

The N2 interface settings specify the properties and connectivity information between this simulated CU range and 5G Core network.

The following table describes the available N2 interface settings that are required for each CU-Simulated range:

Setting	Description
Peer AMF	The IP address of the AMF node connected to (gNodeB) CU over the N2 interface.
Destination port	The destination Stream Control Transmission Protocol (SCTP) port for control plane messages (NG-AP signaling messages) on the N2 interface.
SCTP source port	The source SCTP port for control plane messages (NG-AP signaling messages). Each SCTP endpoint provides the other endpoint with a list of transport addresses through which that endpoint can be reached and from which it will originate SCTP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP port. The default port number is 38412, but you can change it.
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.

Connectivity Settings

The CU-Simulated N2 connectivity settings comprise the interface's IP and MAC addresses and, optionally, outer and inner VLAN identifiers.

- [IP Settings below](#)
- [MAC Settings on the next page](#)
- [VLAN settings on the next page](#)

IP Settings

These settings specify the properties of the F1-UP IP interface.

Setting	Description
IP Address	Enter the IP address for the first simulated CU node in this range. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the simulated CU nodes that are defined in this range will be incremented.
IP Prefix Length	The subnet prefix length associated with this simulated CU IP interface. It specifies the number of leftmost bits in the address, which indicates the network

Setting	Description
	portion of the address.
Gateway Address	This simulated CU node's gateway address towards 5G Core's AMF entity.
Emulated Router Address	Set the IPv4 or IPv6 address for the emulated router (an Xn-U IP interface). The use of the emulated router has the effect of hiding all messages from the interface behind a MAC address. <div>NOTE This option can be used only with IxStack stack.</div>
Emulated Router Address Prefix Length	Set the IP network mask for the emulated router.
Gateway Address	This simulated CU node's first gateway address towards the 5G Core network.
Gateway Address Increment	The value to use when incrementing the Gateway address.

MAC Settings

These settings specify the properties of the F1-UP MAC interface.

Setting	Description
MAC	Specify the first media access control (MAC) address that will be assigned to the eNodeB X2 interface defined in this range. The default value is an auto-generated address that you can change, if desired.
MAC Increment	Specify the value (expressed as a 12-character alphanumeric MAC address value) by which the MAC addresses of all the eNodeB X2 interface defined in this range will be incremented.

VLAN settings

The following VLAN settings are available for the DU-UP F1 interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

N3 Interface Settings

N3 is the user plane interface between the simulated CU and 5G Core network's UPF entity.

The following table describes the available N3 interface settings that are required for each CU-Simulated range:

Setting	Description
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.

Connectivity Settings

The CU-Simulated N2 connectivity settings comprise the interface's IP and MAC addresses and, optionally, outer and inner VLAN identifiers.

- [IP Settings below](#)
- [MAC Settings on the next page](#)
- [VLAN settings on the next page](#)

IP Settings

These settings specify the properties of the F1-UP IP interface.

Setting	Description
IP Address	Enter the IP address for the first simulated CU node in this range. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the simulated CU nodes that are defined in this range will be incremented.
IP Prefix Length	The subnet prefix length associated with this simulated CU IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Port	The UDP port number that will be used for this interface in this range. The default port is 2152 (a registered GTP user plane port).
Emulated Router Address	Set the IPv4 or IPv6 address for the emulated router (an Xn-U IP interface). The use of the emulated router has the effect of hiding all messages from the interface behind a MAC address. <div style="background-color: #f0f0f0; padding: 5px; margin-top: 10px;">NOTE This option can be used only with IxStack stack.</div>
Emulated Router Address	Set the IP network mask for the emulated router.

Setting	Description
Prefix Length	
Gateway Address	This simulated CU node's gateway address towards 5G Core's UPF entity.
Gateway Address Increment	The value to use when incrementing the Gateway address.

MAC Settings

These settings specify the properties of the F1-UP MAC interface.

Setting	Description
MAC	Specify the first media access control (MAC) address that will be assigned to the eNodeB X2 interface defined in this range. The default value is an auto-generated address that you can change, if desired.
MAC Increment	Specify the value (expressed as a 12-character alphanumeric MAC address value) by which the MAC addresses of all the eNodeB X2 interface defined in this range will be incremented.

VLAN settings

The following VLAN settings are available for the DU-UP F1 interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

Xn-C Interface Settings

The Xn-C interface settings specify the properties and connectivity information between this simulated CU range and the gNB-CU under test.

The following table describes the available Xn-C interface settings that are required for each CU-Simulated range:

Setting	Description
Setup Wait Time(ms)	Time to wait (ms) before Xn link setup.

Connectivity Settings

The CU-Simulated Xn-C connectivity settings comprise the interface's IP address and, optionally, outer and inner VLAN identifiers.

- [IP Settings below](#)
- [VLAN settings below](#)

IP Settings

These settings specify the properties of the F1-UP IP interface.

Setting	Description
IP	Enter the IP address for the first simulated CU node in this range. This is the control plane IP address for the simulated CUs for Xn interface. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the simulated CU nodes that are defined in this range will be incremented.
IP Prefix Length	The subnet prefix length associated with this simulated CU IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Port	The SCTP port for XnAP. The default port is 38422.
Gateway Address	This simulated CU node's first gateway address towards gNB-CU device under test.
Gateway Address Increment	The value to use when incrementing the Gateway address.

VLAN settings

The following VLAN settings are available for the DU-UP F1 interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

Xn-U Interface Settings

The Xn-U interface settings specify the properties and connectivity information between this simulated CU range and the gNB-CU under test.

The following table describes the available Xn-U interface settings that are required for each CU-Simulated range:

Setting	Description
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.

Connectivity Settings

The CU-Simulated Xn-C connectivity settings comprise the interface's IP address and, optionally, outer and inner VLAN identifiers.

- [IP Settings below](#)
- [MAC Settings below](#)
- [VLAN settings on the facing page](#)

IP Settings

These settings specify the properties of the F1-UP IP interface.

Setting	Description
IP	Enter the IP address for the first simulated CU node in this range. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses of all the simulated CU nodes that are defined in this range will be incremented.
IP Prefix Length	The subnet prefix length associated with this simulated CU IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Port	The UDP port number that will be used for this interface in this range. The default port is 2152 (a registered GTP user plane port).
Gateway Address	This simulated CU node's first gateway address towards gNB-CU device under test.
Gateway Address Increment	The value to use when incrementing the Gateway address.

MAC Settings

These settings specify the properties of the F1-UP MAC interface.

Setting	Description
MAC	Specify the first media access control (MAC) address that will be assigned to the eNodeB X2 interface defined in this range. The default value is an auto-generated address that you can change, if desired.

Setting	Description
MAC Increment	Specify the value (expressed as a 12-character alphanumeric MAC address value) by which the MAC addresses of all the eNodeB X2 interface defined in this range will be incremented.

VLAN settings

The following VLAN settings are available for the DU-UP F1 interfaces.

Setting	Description
Outer VLAN	Enable this setting if you need VLAN IDs for your test, and then specify the VLAN ID .
Inner VLAN	When <i>Outer VLAN</i> is enabled, DuSIM exposes the optional <i>Inner VLAN</i> setting. Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID .

CHAPTER 13

5G-CORE configuration settings

5G Core is an external entity and can be the device under test (DUT) in a Keysight DuSIM test configuration. Alternatively, the entire 5G Core can be simulated by the Keysight ORAN SIM CE CoreSIM app.



The configuration options are available from the following panels:

- [AMFs panel below](#)
- [AMF panel on the next page](#)

AMFs panel

The AMFs panel opens when you select the 5G-CORE node from the network topology window. You can perform the following tasks from this panel:

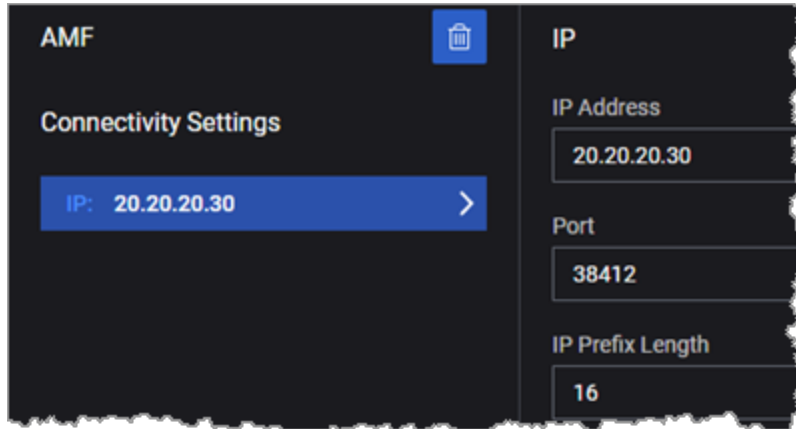
- Add a new AMF to your test configuration.
- Open a AMF configuration for editing or viewing.
- Enable or disable a AMF for the test session.



AMF panel

When you select a node from the AMFs panel, DuSIM opens the AMF panel, from which you can:

- Select the Delete button to delete the selected AMF from the test configuration.
- Select Connectivity Settings to configure the IP addressing and an SCTP port for the AMF.



Connectivity Settings

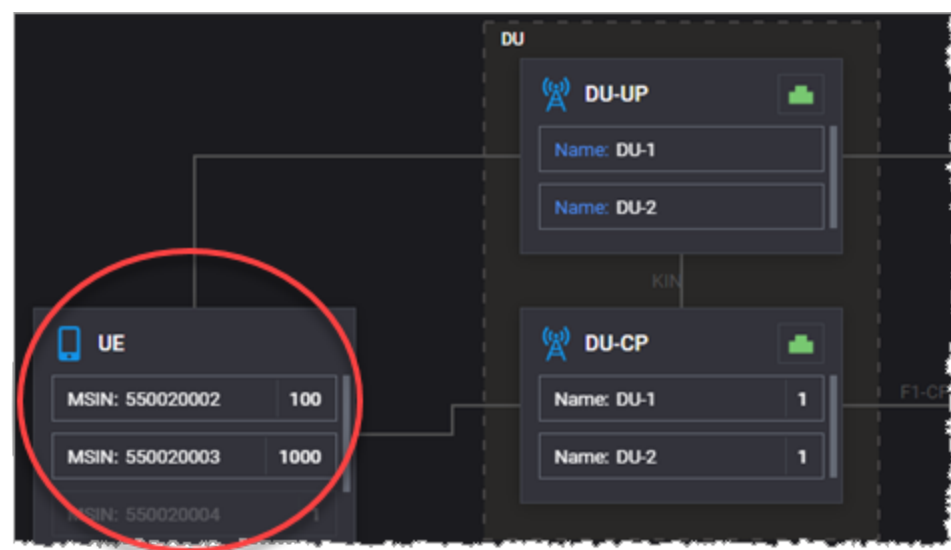
The Connectivity settings specify the properties of the F1-UP IP interface.

Setting	Description
IP	Enter the IP address for this AMF range.
Port	The SCTP port number that will be used for this AMF range. The default port is 38412.
IP Prefix Length	The subnet prefix length associated with this AMF IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

CHAPTER 14

UE configuration settings

When you select the **UE** object from the topology window, DuSIM opens the top-level (leftmost) UE properties window.



The UE properties include all of the settings required to simulate large and varied groups of subscribers who are attempting to access the test network, establish connections to data networks, transmit (and receive) data of various types, and travel amongst the cells contained within your test network.

This chapter describes the UE properties, with the exception of the UE Objectives and UE Scenario Groups, which are described in separate chapters.

The topics in this chapter describe the configuration settings. For procedural instructions, refer to [Configure UEs on page 42](#).

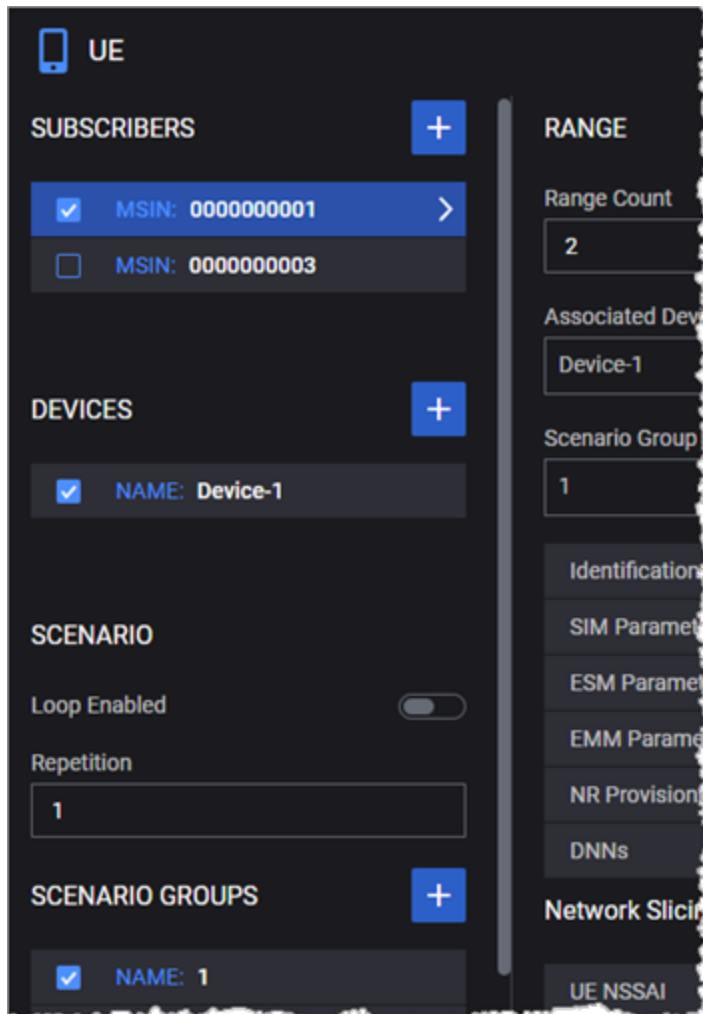
Chapter contents:

UE panel	135
UE RANGE settings	137
Identification settings	138
Subscriber SIM settings	139
Subscriber ESM settings	141
Subscriber EMM settings	143
Subscriber NR Provisioning	145
Subscribers DNN settings	146
Subscriber Network Slicing settings	147

UE Device settings149

UE panel

The **UE** panel opens when you select the UE node from the network topology window. It provides access to several properties panels with which you configure all of the settings needed to simulate one or more ranges of subscribers for your test.



The UE settings are organized as follows:

Subscribers

You configure one or more ranges of subscribers for a test: these are simulated end users, each of which has a unique MSIN. In the UE panel, you can add Subscriber ranges; enable or disable individual Subscriber ranges for your test; and, select a range to configure the settings.

Devices

You configure one or more ranges of UE device types for a test. In the UE panel, you can add UE Device ranges; enable or disable individual Device ranges for your test; and select a range to configure the Device properties.

Scenario

A *Scenario* defines behaviors and actions that are executed by simulated subscribers; each Scenario Group that you configure specifies a unique set of such behaviors. In the UE panel, you can optionally configure looping for the Scenario Groups that are active in the test:

<i>Loop Enabled:</i>	Enable this option if you want the active Scenario Groups to execute continuously throughout the duration of the session.
<i>Repetition:</i>	Specify the number of times that you want the Scenario group to repeat its processing a specific number of times, and then stop.

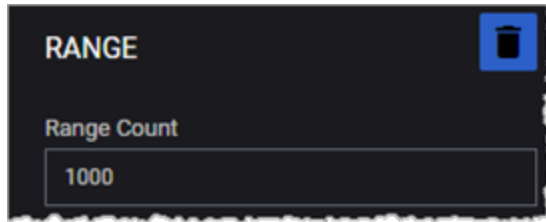
Scenario Groups

In the UE panel, you can add UE Scenario Groups; enable or disable individual Scenario Groups for your test; and select a Scenario Group to configure its settings.

Refer to the following sections for detailed information:


- [UE RANGE settings on the facing page](#)
- [UE Device settings on page 149](#)
- [UE Test Objective settings on page 151](#)
- [Scenario Group settings on page 170](#)

UE RANGE settings



The UE **RANGE** panel provides access to all of the properties that define a UE range.

Except for *Range Count*, all of the other properties are configured on additional panels.

Setting	Description
	Select the Delete Range icon to delete this range from your test configuration.
Range Count	Specify the number of UE to configure for this range.
Associated Device	Select the UE device range (UE Device settings on page 149) that this range of UEs will use.
Scenario Group	Select a Scenario Group for this UE range: each Scenario Group defines the test case scenarios that the UEs in the range will execute during the test run. Refer to Scenario Group settings on page 170 for detailed information.
Detailed subscriber settings	Configure detailed subscriber settings: <ul style="list-style-type: none"> • Identification settings on the next page • Subscriber SIM settings on page 139 • Subscriber ESM settings on page 141 • Subscriber EMM settings on page 143 • Subscriber NR Provisioning on page 145 • Subscribers DNN settings on page 146
Network Slicing	Configure network slicing for this range of UEs: Subscriber Network Slicing settings on page 147 .
Objectives	Configure objectives for this range of UEs: UE Test Objective settings on page 151 .

Identification settings

The Identification properties are assigned to each individual UE in a UE range. Each UE will have a unique MSIN, MSISDN, and IMEI Serial Number value. The MCC and MNC values are shared by all the UEs in a range.

Setting	Description
PLMN MCC	The Mobile Country Code (MCC) for this range of UEs.
PLMN MNC	The Mobile Network Code (MNC) for this range of UEs.
MSIN	The Mobile Subscriber Identification Number (MSIN) to assign to the first subscriber in the range. This value is incremented for each additional subscriber to ensure that each individual subscriber has a unique MSIN.
MSIN Increment	The increment value to create a unique MSIN for each UE in a range. The increment value to use for the second and all subsequent UEs in the range, to ensure that each subscriber has a unique MSIN.
MSISDN	The first Mobile Station ISDN (MSISDN) value in this range.
MSISDN Increment	The increment value to use for the second and all subsequent UE in the range, to ensure that each UE has a unique MSISDN.
IMEI Serial Number	The Serial sequence number (SNR) to use in the construction of the International Mobile Equipment Identity (IMEI) that will be assigned to the UEs in the range. The SNR is a string of six decimal digits.
IMEI Serial Number Increment	The increment value to use for the second and all subsequent UEs in the range, to ensure that each UE has a unique IMEI Serial Number.

Subscriber SIM settings

For each range of subscribers in your test, you configure values that are stored on a mobile device's subscriber identity module (SIM card).


Setting	Description
SMS-Center Address	<p>Enter the SMS center (SMSC) address, using international format. Typically, an SMSC address is a phone number.</p> <p>The E.164 international standard (ITU-T Recommendation) defines a general format for international telephone numbers, in which the number has a maximum of 15 digits (excluding the international call prefix) structured as Country Code + Subscriber Number. Country Code contains no more than three digits and the Subscriber Number contains no more than 12 digits.</p> <p>An SMS (short message service) center handles the SMS operations of a wireless network. When a UE sends an SMS message, that message is first directed to an SMS center. The SMS center then forwards the SMS message towards the destination.</p> <p>The standard practice is for the wireless network operator to preset the SMSC address in the SIM card.</p>
LTE Authentication Algorithm	<p>Use this parameter to select the LTE authentication algorithm used by the UE range. You can select from among the following options:</p> <ul style="list-style-type: none"> • Milenage – OPc set: Milenage algorithm set with OPc; both the Authentication key and Authentication OPc parameters are required. • Milenage – OPc set: Milenage algorithm set with OP; both the Authentication key and Authentication OP parameters are required. • Test Algorithm: test algorithm for authentication, as defined in 3GPP TS 34.108; only the Authentication key parameter is required. <p>For additional details, refer to TS 35.206 for Milenage algorithm and TS 24.108 sub-clause 8.1.2 for Test algorithm.</p>
LTE Authentication Response Parameter	<p>Enter the numeric value (RES) that will be included in the IE Authentication response parameter in the AUTHENTICATION RESPONSE message.</p>
Authentication Key	<p>Enter the Authentication key value for the simulated subscriber identity module in this subscriber range.</p> <p>This is a 16-byte hexadecimal string, as described in 3GPP TS 33.401, subclauses 6.1 and 6.2.</p>
Authentication OP/OPc	<p>Enter the Authentication OP or OPc value for the simulated subscriber identity module in this subscriber range. (Either OP or OPc is stored on the SIM card, depending upon how an operator chooses to implement it.)</p> <p>This is a 16-byte hexadecimal string, as described in 3GPP TS 35.206, subclauses 2.3 and 5.1.</p>

Setting	Description
LTE Authentication Response Parameter Length	Enter the desired length of the authentication response (RES) value. The valid length range is from 4 octets through 16 octets.
Main Access Class	<p>Enter the desired main access class for this Subscriber range; the valid range is zero through nine.</p> <p>The 3GPP defines sixteen Access Classes for controlling access to the air interface. These classes establish a basic distinction between emergency sessions, high-priority users, and standard users.</p>
Force High Priority Access Establishment	<p>If the Subscriber range requires high-priority access establishment, select this option and then choose the specific class:</p> <ul style="list-style-type: none"> • 11 – For PLMN use • 12 – For security services • 13 – For public utilities • 14 – For emergency services • 15 – For PLMN staff

Subscriber ESM settings

The EPS Session Management (ESM) protocol supports the establishment and handling of user data sessions in the Non-Access Stratum (NAS). This includes the establishment of Packet Data Network (PDN) connections and EPS bearers for the UEs accessing the network.

For each range of subscribers in your test, you configure ESM values that are needed when establishing subscriber sessions with the network.

Setting	Description
Request Type	<p>Select the ESM Request Type for this subscriber range:</p> <ul style="list-style-type: none"> Initial Attach: Initial network attachment request. Handover: Requests a transfer of a PDN connection from non-3GPP access to 3GPP access (and vice versa). Emergency: Requests establishment of an emergency connection. Initial Request: Requests establishment of connectivity to a PDN for the first time. <p>The Request Type information element is described in TS 24.008, subclause 10.5.6.17.</p>
Packet Data Network Type	<p>Select the PDN Type to place in the PDN Type information element for this subscriber range: IPv4 Supported, IPv6 Supported, or IPv4V6 Supported.</p> <p>The purpose of the PDN Type information element is to indicate the IP version capability of the IP stack associated with the UE (as specified in TS 24.301, subclause 9.9.4.10).</p>
Access Point Name	<p>Enter the Access Point Name that will be placed in the Access Point Name information element for the subscribers in the range. The Access Point Name IE identifies the packet data network to which the subscriber wishes to connect.</p>
Protocol Configuration Options	<div data-bbox="423 1285 849 1344">  Configure </div> <p>Click the Configure button if you need to configure Protocol Configuration Options (PCOs) for this Subscriber range. DuSIM will open the floating Protocol Configuration Options dialog in which you will configure the PCOs (refer to Protocol Configuration Options dialog on the next page).</p> <p>These values are placed in the Protocol Configuration Options information element. The options are described in TS 24.008, Table 10.5.154. The purpose of the Protocol Configuration Options information element is to transfer external network protocol options associated with a PDP context activation.</p>
ESM Information Transfer Flag	<p>Select one of the available options for the ESM Information Transfer Flag information element:</p> <ul style="list-style-type: none"> Enabled: Send the ESM Information Transfer Flag IE, with the value set to 1. Disabled: Send the ESM Information Transfer Flag IE, with the value set to 0.

Setting	Description
	<ul style="list-style-type: none"> • Not included: Do not send the ESM Information Transfer Flag IE. <p>The UE will include the ESM Information Transfer Flag IE in the PDN CONNECTIVITY REQUEST message sent during the attach procedure if the UE has protocol configuration options that need to be transferred (with security protection) or wants to provide an access point name for the PDN connection to be established during the attach procedure.</p> <p>The ESM Information Transfer Flag is described in TS 24.301, subclauses 8.3.20.2 and 9.9.4.5.</p>
PDU Session ID	<p>Enter the PDU Session ID for this range.</p> <p>Every PDU Session Establishment Request message sent to the network by a UE includes a PDU Session ID. The PDU Session ID is unique per UE and it is the identifier used to uniquely identify one of a UE's PDU Sessions.</p>

Protocol Configuration Options dialog

If you click the **Configure** button in the *Protocol Configuration Options* field of the Subscriber ESM Parameters properties panel, DuSIM opens the **Protocol Configuration Options** dialog. You use this dialog when you need to configure Protocol Configuration Options (PCOs) for this Subscriber range: a PCO list and/or an Additional Parameters List.

Please contact Technical Support for assistance with this option.

Subscriber EMM settings

For each range of subscribers in your test, you configure EPS Mobility Management (EMM) values that specify the required support and options for attach and detach procedures.

A UE attaches to a network by exchanging Non-Access Stratum (NAS) control signaling messages with the network. EMM encompasses the NAS procedures related to subscriber network attachment and mobility. These procedures include (among others) Attach, Detach, and Tracking Area Update (TAU).

Setting	Description
Attach Type	<p>Select the Attach Type value for the Attach procedures that the subscribers in the range will request.</p> <ul style="list-style-type: none"> • EPS Attach: The UE requests an EPS attach. • Combined EPS-IMSI Attach: The UE requests a combined EPS/IMSI attach and informs the network that the UE is capable of and configured to use CS fallback and/or SMS over SGs. • EPS Emergency Attach: The UE requests an EPS Emergency attach.
Detach Type	<p>Select the type of Detach procedure that the subscribers in the range will request.</p> <ul style="list-style-type: none"> • EPS Detach: The UE requests an EPS-only detach. • IMSI Detach: The UE requests an IMSI-only detach. • EPS IMSI Detach: The UE requests a combined EPS/IMSI detach.
Switch-Off at Detach	<p>When this option is enabled, the DETACH REQUEST message sent by the UE will contain the Detach type IE which indicates that the detach is due to a "switch off". In this case, the procedure is completed when the network receives the DETACH REQUEST message.</p>
Extended Periodic Timers Supported	<p>When this option is enabled, the UE will include the MS Network Feature Support IE in the Attach Request message to indicate support for extended periodic timer value.</p>
Enable Timer 3412 extended value	<p>When this option is enabled, the UE will request support for a particular T3412 value by including the T3412 Extended Value IE in the Attach Request message.</p> <p>If the network supports this feature, it may include the T3412 Extended Value IE in the Attach Accept message to provide the UE with a longer periodic tracking area update timer.</p>
Timer 3412 extended value	<p>Enter the Timer 3412 extended value. This is an integer in the range 0-31.</p> <p>The value is placed in the GPRS Timer 3 information element. The purpose of this IE is to specify GPRS specific timer values. Refer to TS 24.008, subclause 10.5.7.4a for additional detailed information.</p>
Attach Without PDN	<p>When this option is enabled, the UE specifies—in the Preferred Network Behaviour indication—that Attach Without PDN Connectivity is supported.</p>

Setting	Description
Enabled	When Attach Without PDN Connection is supported, the UE need not establish a PDN connection as part of the Attach procedure and the UE and MME may at any time release all the PDN connections and remain EPS-attached.
Force PLMN	Enable this option if you wish to configure the Public Land Mobile Network (PLMN) codes for this range. When it is enabled, the <i>Force MCC</i> and <i>Force MNC</i> fields are made available for configuration.
Force MCC	Enter the MCC (Mobile Country Code) for this range. This field is available for configuration only if <i>Force PLMN</i> is enable.
Force MNC	Enter the MNC (Mobile Network Code) for this range. This field is available for configuration only if <i>Force PLMN</i> is enable.
Enable eDRX	Select this option to enable eDRX for this subscriber range. When it is enabled, the <i>PTW WB-S1</i> , <i>eDRX S1</i> , and <i>Paging eDRX CRC Type</i> fields are made available for configuration.
PTW WB-S1	Enter the Paging Time Window (PTW) value for WB-S1 Mode, as defined in TS 24.008. The valid values range from zero through 15.
eDRX S1	Enter the value eDRX Value for S1 Mode (extended idle mode DRX cycle length), as defined in TS 24.008. The valid values range from zero through 15.
Paging eDRX CRC Type	Select the algorithm to use for computing the P-HSFN, starting from the UE identity. The default algorithm is CRC-32. The other option is crc32-bzip2.

Subscriber NR Provisioning

In the **NR Provisioning** settings, for each subscribers range, you configure the routing indicator (RI), the Serving Network Name, the Home Public Key ID, and the protection scheme ID.

About SUPI and SUCI ...

- **SUPI:** In the 5G system, the SUBscription Permanent Identifier (SUPI) is a globally unique identifier allocated to each subscriber. The serving network must authenticate the SUPI in the process of authentication and key agreement between UE and network. The serving network authorizes the UE through the subscription profile obtained from the home network; this UE authorization is based on the authenticated SUPI.
- **SUCI:** The SUPI is never transferred in clear text over the 5G-RAN; instead, the SUCI is used. the SUBscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed SUPI. In the 5G core network, only the UDM has authority to deconceal the SUCI. For detailed information, refer to 3GPP TS 33.501 (Security architecture and procedures for 5G System).

Setting	Description												
Routing Indicator	<p>The Routing Indicator that is used in the construction of the SUCI.</p> <p>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and is provisioned in the USIM.</p>												
Serving Network Name	<p>The name of the serving network that will authenticate the SUPI in the process of authentication and key agreement between the UE and the network.</p>												
Home Network Public Key ID	<p>The Home Network Public Key Identifier that will be used to indicate which public/private key pair to use for SUPI protection and deconcealment of the SUCI.</p>												
Protection Scheme ID	<p>Select the desired SUCI Protection Scheme for the subscribers in the range. The available schemes are those listed in TS 33.501, Annex C.</p> <table><tr><th>Scheme</th><th>Identifier</th><th>Size of the scheme output</th></tr><tr><td>null-scheme</td><td>0x0</td><td>Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)</td></tr><tr><td>Profile-A</td><td>0x1</td><td>Total of 256-bit public key, 64-bit MAC, and size of input</td></tr><tr><td>Profile-B</td><td>0x2</td><td>Total of 264-bit public key, 64-bit MAC, and size of input.</td></tr></table>	Scheme	Identifier	Size of the scheme output	null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)	Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input	Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.
Scheme	Identifier	Size of the scheme output											
null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)											
Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input											
Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.											

Subscribers DNN settings

For each range of subscribers in your test, you select at least one Data Network Name (DNN) from the pool of DNNs that have been configured for the test. These DNNs are the data networks to which subscribers establish connections during test execution.

Prerequisite

Before selecting DNNs for subscriber groups, you need to configure a pool of DNNs in the **Global Settings**.



Selecting DNNs for subscribers

To select DNNs for a subscriber range:

1. Select the range from the UE **SUBSCRIBERS** panel.
2. In the Subscribers **RANGE** panel, select **DNNs**.
DuSIM opens the **DNNs** panel, from which you can add, delete, and select DNNs for the selected range of subscribers.
3. To select a DNN value for one of the entries in the **DNNs** list:
 - a. Select the desired **DNNs** entry (they are numbered sequentially, starting with 1).
DuSIM displays the selected entry in the **DNN** panel.
 - b. Select the desired DNN value from the **DNN** drop-down list.
4. To add another DNN to the subscriber range:
 - a. Click the **Add DNN** button in the **DNNs** panel.
 - b. Select the desired DNN from the **DNN** drop-down list.

DNN settings

The DNN settings establish a mapping between DNNs and UE IPs, thereby enabling multiple PDU sessions for each subscriber in the range.

Setting	Description
<i>DNNs:</i>	
	The following actions are available: <ul style="list-style-type: none"> • Select the Add DNN button to add a new DNN for the selected subscriber range. • Select a DN from the list to access the configuration settings.
<i>DNN settings:</i>	
	Select the Delete DNN button to remove this DNN from the selected subscriber range configuration.
DNN	Select one of the previously-defined DNNs from the drop-down list.

Subscriber Network Slicing settings

The UE Network Slicing settings configure one or more NSSAIs for a selected subscriber range.

To access the settings

To access the Network Slicing settings for a subscriber range:

1. Select the range from the UE **SUBSCRIBERS** panel.
2. In the Subscribers **RANGE** panel, select **UE NSSAI**.



DuSIM opens the **UE NSSAI** panel, from which you can add, delete, and configure UE NSSAIs for the selected range of subscribers.

UE NSSAI settings

Each UE Subscriber range requires at least one NSSAI range. These are Requested NSSAIs that are signaled (in NAS messages, including Registration and PDU Session Establishment) by the UE to the network. They enable the network to select the Serving AMF, Network Slice(s), and Network Slice instance(s) for the UE.

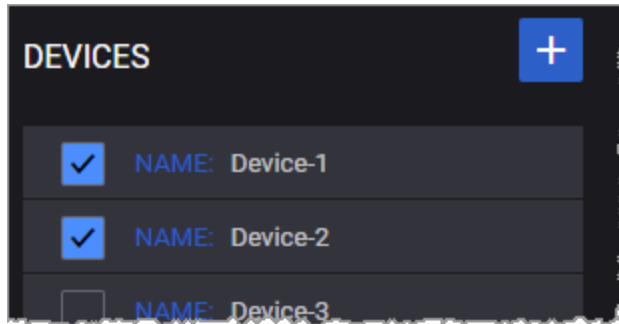
The S-NSSAI information element includes a mandatory Slice/Service Type (SST) field, an optional Slice Differentiator (SD) field, and it can also include an optional Mapped Configured SST and an optional Mapped Configured SD.

The following table describes the **UE NSSAI** settings.

Setting	Description
<i>UE NSSAI:</i>	
	<p>The following actions are available:</p> <ul style="list-style-type: none"> • Select the Add UE NSSAI button to add a new UE NSSAI to your test configuration. • Select a UE NSSAI from the list to access the configuration settings.
<i>UE NSSAI settings:</i>	
	Select the Delete UE NSSAI button to delete this UE NSSAI from your test configuration.
SST	<p>The value that identifies the SST (Slice/Service Type) for this S-NSSAI. SST comprises octet 3 in the S-NSSAI information element. The standardized SST values are:</p> <ul style="list-style-type: none"> 1 (eMBB) 2 (URLCC) 3 (MIoT)
SD	<p>The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.</p>

Setting	Description
Mapped SST	The Mapped configured Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this S-NSSAI.

UE Device settings



Each Subscriber range selects a **Device** range, and each Device range defines the properties of a specific type of mobile device.


To define your device ranges, select **UE** from the topology window, and then add and configure the Device ranges that you will use in your test.

When you select a device range from the UE **DEVICES** pane (such as *Device-1* in the above example), DuSIM opens the properties panel for that range, which provides access to the device configuration settings.

- [Device settings below](#)
- [ULRRC Parameters below](#)
- [EMM Parameters on the next page](#)

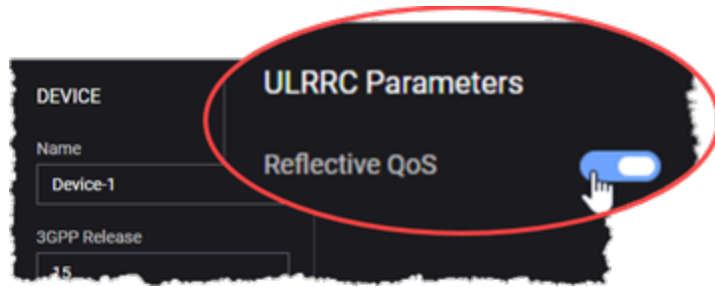
Device settings

The following table describes the UE **Device** settings.

Setting	Description
	Select the Delete Range icon to delete this range from your test configuration.
Name	A name that identifies the specific device.
3GPP Release	The 3GPP Release that the device supports.
IMEI TAC	The Type Allocation Code (TAC) assigned to the device model.
Software Version	The Software Version value identifies the IMEI Software Version Number (SVN) that is incorporated into the IMEI, as the final two digits. It indicates the software (or firmware) version that is present on the device.

ULRRC Parameters

There is a single uplink (UL) Radio Resource Control (RRC) device setting: *Reflective QoS*.



Reflective QoS can be enabled or disabled for each UE device that you define for the test. When you enable the option, any UE using that device configuration will indicate to the SMF that it supports Reflective QoS during PDU Session Establishment.

When enabled, the UE takes the QoS that is applied in the downlink and applies it to the uplink traffic. Refer to 3GPP TS 23.501 for detailed information.

EMM Parameters

Each device requires the following EPS Mobility Management (EMM) parameters. EMM encompasses the NAS procedures related to subscriber network attachment and mobility.

Parameter	Description
UE Network Capability	A hex string that specifies the encoded UE network capabilities of the device. The default value is e0c0e0e0.
UE Security Capability	A hex string that specifies the encoded UE security capabilities of the device. The default value is 80800000.

CHAPTER 15

UE Test Objective settings

In a DuSIM test, an *objective* is a set of performance and event targets that the test is attempting to achieve. The objectives are individually configured for a given UE range. A test, therefore, may have multiple UE ranges each of which is attempting to achieve a specific set of objectives.

Each UE range defines its own test objectives. The objectives specify the properties of the application traffic that the UEs in the range will generate and transmit over the user plane. Each range can create more than one type of application traffic, and for each type, you configure one of the available objective types. The objective types include throughput, concurrent connections, and connection rate.

As an example, for a given UE range, your test objective may be to achieve a 10 Gb throughput rate. For this objective, your test will select and configure an application type—such as HTTPS Get or FTP—and will configure all of the properties that enable simulation of realistic application traffic in your test network.

Chapter contents:

User Plane panel	152
Stateless UDP Traffic	154
Data Traffic	155
Voice Traffic	158
Video OTT	163
DNS Client Traffic	164
UDG Traffic	166

User Plane panel

The User Plane Objectives focus on the rate and volume of user plane traffic that the simulated UEs are sending to the network. You define separate User Plane objectives for each UE subscriber range. Based on your test requirements, the configuration of the User Plane Objectives involve settings for the traffic generators on the UE.

- [Accessing the User Plane Objectives](#)
- [Application Traffic settings below](#)

Accessing the User Plane Objectives

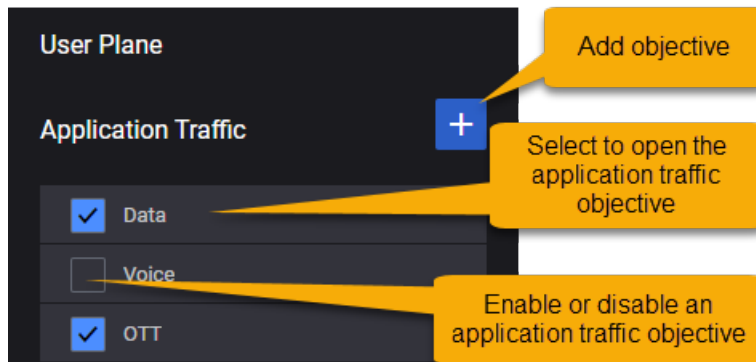
To access the User Plane Objectives:

1. Select the **UE** panel, then select a Subscriber. This opens the UE **Range** panel.
2. In the Range panel, click **User Plane** in the Objectives section.
This opens the **User Plane** panel.



From the **User Plane** panel, you can add additional traffic applications and access the properties panels for traffic applications that are already defined.

Application Traffic settings

From the User Plane panel, you can add, select, enable, and disable objectives.



The following table describes the Application Traffic generation parameters.

Parameter	Description
	Click the Add Objective button to add a new add a new application traffic objective.
	Click the Delete Objective button to remove the application traffic objective from your test configuration. <i>This button is available when you select the application traffic objective and you open the properties panel.</i>
Application Type	Select the type of traffic you want to generate. The available traffic applications are:

Parameter	Description
	<ul style="list-style-type: none">• Stateless UDP• Data• Voice• Video OTT• DNS Client• UDG <p><i>This field is available when you select the application traffic objective and you open the properties panel.</i></p>

Stateless UDP Traffic

Use the **Stateless UDP** generator if you want to generate IP packets that encapsulate UDP payload. The Stateless UDP generator configuration settings for the uplink traffic are described below.

The following table describes the Stateless UDP parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Flow Type	This field cannot be modified.
Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The time to wait before the application traffic flows start.
Destination IP Address	The destination IP address to place in the IP packet.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNNs Settings on page 55 .
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before the application traffic flows start.
IP Preference	Select the IP address preference: IPv4 or IPv6 .


Data Traffic

The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Throughput • Concurrent Connections • Connections Rate
Throughput (kbps)	This parameter is available only when Objective Type is set to Throughput . The desired maximum throughput (in kbps) for the combined traffic flows that will be generated.
Concurrent Connections	This parameter is available only when Objective Type is set to Concurrent Connections . The maximum number of concurrent data traffic connections.
Connection duration (sec)	This parameter is available only when Objective Type is set to Concurrent Connections . The maximum duration for each data traffic connection.
Connections rate per second	This parameter is available only when Objective Type is set to Connections Rate . The maximum number of connections per second.
Connection multiplier (per UE)	Set the value for the connection multiplier.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before the application traffic flows start.
IP Preference	Select the IP address preference: IPv4 or IPv6 .

Application Traffic Flows

You can add and delete traffic flows as needed to meet your test objectives. The Application Traffic Flow parameters are described in the following table.

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Type	<p>Select the L4/L7 protocol type from the list of pre-defined flows. The available types include:</p> <ul style="list-style-type: none"> • HTTP GET, HTTP PUT, and HTTP POST • HTTPS GET, HTTPS PUT, and HTTPS POST • FTP • UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)
Port	The server (destination) port used by the flow.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or HTTPS server.
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional .
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional .
URL	The URL that is being accessed by the flow's protocol.
Destination Hostname	Destination hostname of the server. If DNS hostname resolution is enabled for the flow and Name Servers are configured under Global Settings, this name will be resolved before being used as L7 destination IP for the flow and included in HTTP headers. If empty, the "Address" from the previous fly-out level will be used as L7 destination IP for the flow.
Close TCP Connection After Each Transaction	Select the check-box to terminate the TCP connection after each transaction.
Enable DNS	Select the check-box to process only one DNS query per TCP connection.

Parameter	Description
Query Per Connection	
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (Subscribers DNN settings on page 146).

Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Throughput (kbps)	This parameter is available only when Objective Type is set to Throughput . The desired maximum throughput (in kbps) for the combined traffic flows that will be generated.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before the application traffic flows start.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Call Type	Select the type of call from the drop-down list. Available options are: <ul style="list-style-type: none"> • Basic Call • Basic Call Mo (Mobile Originated) • Basic Call Mt (Mobile Terminated)
Dial Plan	For the settings required to configure the dial plan, refer to Dial Plan on the facing page .
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by DuSIM or overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPsec.
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by DuSIM or overwrite it with your own value.



Parameter	Description
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select this option in order to enable RTCP.
<i>Media settings:</i>	<i>For the configuration of media settings, refer to Media Settings on the next page.</i>

Dial Plan

The parameters required to configure the dial plan are presented in the table below.

Parameter	Description
DNN ID	Select the DNN from the drop-down list.
Iterations	The number of times the Voice flow will be executed. It can be finite or infinite (set to zero).
UPDATE	Select this button in order to update IMSI and Source Phone with UE range identification settings.
IMSI	Read-only field, it displays the updated IMSI.
IMSI Phone Increment	The value by which the IMSI phone number is incremented.
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.
Source Phone Increment	The value by which the destination phone number is incremented.
Destination IP	The destination IP address.
Destination IP Increment	The value by which the destination IP is incremented.
Destination Port	The destination port number.

Media Settings

Parameter	Description
Media Duration (ms)	Length of time to play the media stream. You can accept the value provided by DuSIM or overwrite it with your own value.
Enable Video	If selected, video traffic is enabled.
<i>Jitter Buffer Settings:</i>	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
<i>Audio Codecs</i>	
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	<p>Select the audio codec from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • AMR/AMR-WB on the facing page - The Adaptive Multi-Rate (AMR) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • AMR/AMR-WB on the facing page - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • EVS on the facing page - The EVS (Enhanced Voice Services) codec specified by 3GPP TS 26.445 compresses 20ms input blocks of audio samples. In addition to the EVS Primary mode, 3GPP TS 26.445 specifies that the codec implement the EVS AMR-WB IO mode for interoperability with AMR WB devices. • PCMU/PCMA/iLBC/G722/G723/G729 on page 162 • PCMU/PCMA/iLBC/G722/G723/G729 on page 162 • PCMU/PCMA/iLBC/G722/G723/G729 on page 162 • PCMU/PCMA/iLBC/G722/G723/G729 on page 162 • PCMU/PCMA/iLBC/G722/G723/G729 on page 162 • PCMU/PCMA/iLBC/G722/G723/G729 on page 162 <p>The parameters of each audio codec are presented below.</p>

AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> • Bandwidth efficient: In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added. • Octet aligned: In the octet-aligned format, all the fields in a payload, including payload header, table of contents entries, and speech frames themselves, are individually aligned to octet boundaries to make implementations efficient. All fields of an AMR payload (payload header, table of contents and speech) are individually octet aligned.
Bitrate	<p>Indicates the mode (bitrate) of the AMR codec.</p> <p>For AMR there are eight available modes. All these modes can be changed dynamically without negotiation, reflecting the main characteristics of this codec – adaptive rate.</p> <p>For AMR WB there are nine modes available.</p>

EVS

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet.
Payload Type	Specifies the audio payload type.
Payload Format	<p>The following options are available:</p> <ul style="list-style-type: none"> • Header full - In this payload format, the payload consists of one or more coded frame(s). The packet headers contain the Table of Contents (ToC) byte(s) and the Change Mode Request (CMR) byte. • Compact - In this payload format a single codec data frame is sent in each RTP packet. The format uses protected payload sizes that uniquely identify the EVS codec bitrates for the EVS Primary or EVS AMR-WB IO mode.
Bitrate	Indicates the mode(bitrate) of the EVS codec. Select the value from the drop-down list.

PCMU/PCMA/iLBC/G722/G723/G729

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet.
Payload Type	Specifies the audio payload type.

Video OTT

The following table describes the OTT (Over-the-Top) traffic parameters.


Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none">• Simulated Users• Throughput
Throughput	The desired maximum throughput (in kbps) for the video traffic flow that will be generated.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start.

DNS Client Traffic

The following table describes the DNS Client Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to DNS Client .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Connection multiplier (per UE)	Set the value for the connection multiplier.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Application Traffic Flows	<p>Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"> • To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings. • To add another traffic flow, click the Add Flow button. DuSIM will open the Flow panel where you will select the flow type and configure the flow settings. <p>Refer to Application Traffic Flows on the facing page (below) for a description of the configuration settings for these traffic flows.</p>

Application Traffic Flows

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Type	By default, the type is set to DNS Client .
Port	The port used by the flow.
DNS Server IP	Set the DNS server IP address.
Number of DNS servers	Set the number of DNS servers.
Hostname	Set the hostname.
Query Type	<p>Defines the type of information that will be requested from the DNS Server. Select the query type from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • A - An address mapping (A) record is a DNS record which stores a hostname and its corresponding IPv4 address. • AAAA - An AAAA record is a DNS record that contains the IPv6 address for a domain. • CNAME - A Canonical Name (CNAME) record is a type of DNS resource record that maps one domain name (an alias) to another (the canonical name). • TXT - A text (TXT) record is a type of DNS record that contains text information for sources outside of the domain and also carries machine-readable data such as encryption, sender policy, etc. • PTR - A Reverse-lookup pointer (PTR) record is a DNS record type used for reverse IP lookups. • NS - The name server (NS) record is a type of DNS record that specifies the domain name of the name server.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNsSettings)

UDG Traffic

The following table describes the User Data Generator (UDG) Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to UDG .
Label	Assign this traffic instance a unique label.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before starting the application traffic flows.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
TCP Settings	Refer to TCP Settings below below.
UDP Settings	Refer to UDP Settings on the facing page below.
<i>Traffic Flow:</i>	
Application Traffic Flows	Each UDG Application Traffic entry requires UUDG traffic flow entry. UUDG is the UDG client on the UE side. Refer to Traffic Flow on page 168 for descriptions of the UUDG traffic flow settings below.

TCP Settings

The following table describes the UDG Application Traffic TCP settings.

Setting	Description
Min Retransmission Timeout (ms)	The lowest value (in ms) to which the computed RTO timer value can be set. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max Retransmission Timeout (ms)	The highest value (in ms) to which the computed RTO timer value can be set.
Receive Buffer Size	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.

Setting	Description
Transmission Buffer Size	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	Enable this option to enable the Selective Acknowledgment (SACK) option in the TCP packets.

UDP Settings

The following table describes the UDG Application Traffic UDP settings.

Setting	Description
Receive Buffer Size	The default size of the receive buffer (in bytes). This parameter affects the UDP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmission Buffer Size	The default size of the transmit buffer (in bytes). This parameter affects the UDP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).

Traffic Flow

The following tables describes the UUDG traffic flow settings.

- [Flow below](#)
- [UDG Traffic Parameters below](#)

Flow

The following settings are configured on the **Flow** panel, once you select UUDG from the UDG Application Traffic panel.

Parameter	Description
Transport Protocol	Select the desired transport protocol to use for this UUDG traffic flow: TCP or UDP..
Out of Band Signaling	Select this option to allow the UDG signaling to be carried on a different path with respect to the data path, directly between the UUDG (UDG client on the UE side) to the NUDG (UDG Network side peer). When you enable this option, DuSIM opens an Out of Band Signaling panel in which you specify the address values for the out of band channel.
Destination Hostname	The IP address or host name of the traffic flow destination.
Port	The server (destination) port used by the flow.
Reconnect Timeout (ms)	Specify the reconnection timeout value (in milliseconds) for this traffic flow. This is the time interval after which the client attempts to reconnect after the connection was interrupted. A value of zero means that reconnect is disabled.
DNN ID	Select the DNN for this flow. The DNNs are configured in the DNNs Settings on page 55 .

UDG Traffic Parameters


The following table describes the UDG traffic parameters that need to be set for this traffic flow.

Parameter	Description
UDG Test Type	Select the UDG test type: <ul style="list-style-type: none"> • Ping-Pong: the test procedure allows uplink and downlink ping packets. • Transmission: the test procedure allows transmit data packets.
<i>Transmission</i>	
Client Burst Interval (ms)	The number of milliseconds between client traffic bursts.
Client Burst size	The number of packets to include the each client traffic burst.

Parameter	Description
(packets)	
Client Packet Size (bytes)	The size of each of packets included in the client traffic bursts.
Server Burst Interval	The server traffic burst interval (enter a numeric value).
Server Burst Interval Unit	Select Milliseconds or Microseconds.
Server Burst size (packets)	The number of packets to include the each server traffic burst.
Server Packet Size (bytes)	The size of each of packets included in the server traffic bursts.
<i>Ping-pong</i>	
Ping Direction	Set the ping direction. Available options: Upstream or Downstream .
Ping Interval	Enter the numeric interval value.
Ping Interval Unit	Set the ping interval unit. Available options: Millisecond or Microsecond .
Pong Number	The number of pong packets to receive for a ping packet.
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.

CHAPTER 16

Scenario Group settings

 You access the Scenario Groups settings from the top-level (leftmost) **UE** property panel. From this panel, you can add additional Scenario Groups and access the properties panels for Scenario Groups that are already defined. This section describes Scenario Group procedure settings: for information about creating Scenario Groups, refer to [Create Scenario Groups on page 34](#) for detailed instructions.



A DuSIM *Scenario Group* comprises a set of *test suites* that the test will perform. For each test suite, you configure a procedural call flow: the procedures that will be sequentially initiated when the test starts. The procedures include Registration, Session Establishment, among others. For each procedure that you include in a call flow, you configure properties that simulate realistic network access behavior for the simulated subscribers in the test.

Once you have created the Scenario Groups that you need for the test, you will configure each UE range to choose one or more of the Scenario Groups. Each UE range can use any of the available Scenario Groups, and a Scenario Group can be used by more than one UE range.

Whereas the configured Test Objectives define the detailed properties of the simulated *user plane* traffic for the test, the Scenario Groups define the detailed *control plane* traffic that enables the subscribers to access the network and successfully transmit user plane traffic.

Chapter contents:

Mobility settings	172
Test Suite settings	175
Test procedures for SA	176
Deregistration	177
PDU Session Establish	178
PDU Session Release	180

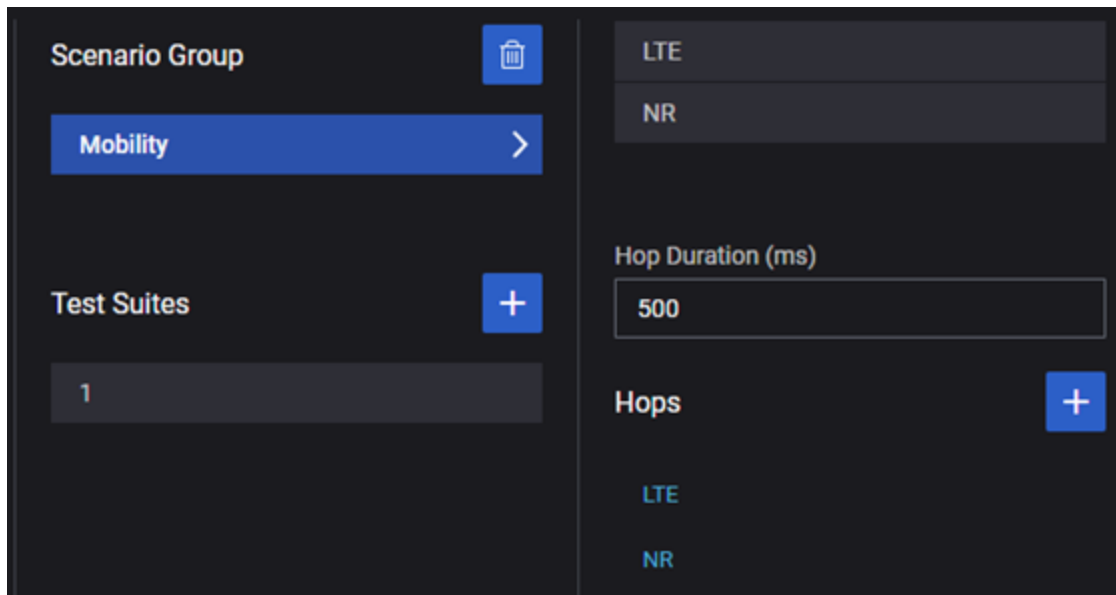
Registration	182
Service Request	183
Test procedures for NSA tests	184
Attach	185
Detach	186
ENDC Configuration Update	187
EPS Bearer Activation	188
EPS Bearer Deactivation	189
Inter eNB Handover	190
PDN Connection Activation	191
PDN Connection Deactivation	193
SCG Release	195
SGNB Addition	196
Test procedures for SA and NSA	198
Application Traffic	199
Delay	200
DU Initiated Release	201
NR-U Modification Request	202

Mobility settings

This topic describes the configuration settings required for UE mobility events. For step-by-step instructions for configuring mobility, and for additional information about the mobility operation, refer to [Configure mobility on page 36](#) (in the [Build and run a test on page 18](#) chapter).

You define UE mobility for each Scenario Group. When a given Scenario Group is selected for a UE range, the UEs in that range perform the mobility actions, as configured in the Mobility settings.

To access the mobility configuration settings, click **Mobility** from the **Scenario group** properties panel.



Mobility properties

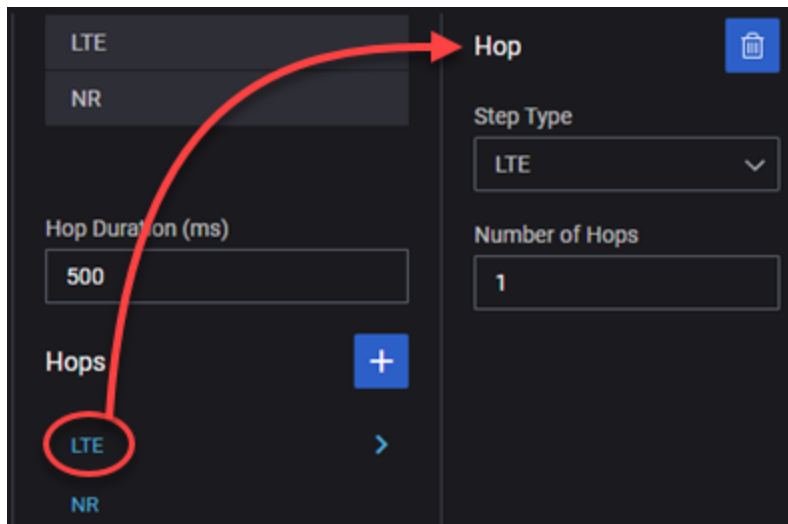
These are the settings that appear in the panel that opens when you select **Mobility** from the Scenario Group panel.

Setting	Description
<i>LTE Settings:</i>	
LTE	Click LTE to open the mobility event settings in a new panel.
eNodeB	Select the eNodeB range in which the mobility actions start.
Strategy	Select the type of mobility handover event: <ul style="list-style-type: none"> • Intra eNB: The UE moves from one sector to another sector that is managed by the same eNB. • Inter eNB: The UE enters the eNB's cell from a neighboring eNB cell. The UE leaves a cell managed by the eNB and enters a cell managed by a second eNB, within the same E-UTRAN.


Setting	Description
<i>NR Settings:</i>	
NR	Click NR to open the mobility event settings in a new panel.
DU	Select the DU range in which the mobility actions start.
Strategy	Select the desired handover procedure <i>Strategy</i> : <ul style="list-style-type: none"> • Intra DU: The UE moves among cells in the same DU. • Inter DU: The UE moves between cells in different DUs. • Inter CU: The UE context is transferred from a source CU to a target CU, over the Xn interface.
<i>Hop settings:</i>	
Hop Duration	The number of milliseconds to wait between successive hops in the mobility path.
Hops	Click the Add Hop button to add a hop instance. DuSIM adds an <i>NR</i> instance to the panel. When you click the instance, DuSIM opens the Hops panel below . The instance name is automatically created as NR . But if you change the <i>Step Type</i> to LTE in the Hops panel, DuSIM changes the instance name to reflect that step type.
NR and LTE	When you click the Add Hop button, DuSIM adds a hop instance, which is named NR by default. The name will change to LTE if you change that instance's <i>Step Type</i> in the Hops panel. Clicking these instance names opens their configuration panels for editing, as described in Hops panel below .

Hops panel

When you select a hop instance from the Mobility properties panel, DuSIM opens the Hops panel.

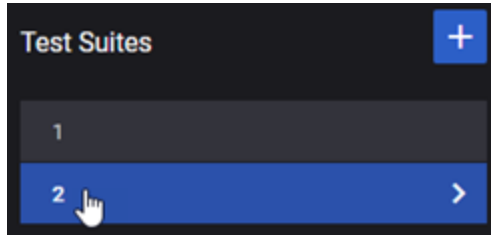


The following table describes the configuration settings in the Hops panel.

Setting	Description
	Delete this hop instance from the configuration.
Step Type	Select NR if the UE is moving within a 5G network, or LTE if the UE is moving within a 4G network.
Number of Hops	Enter the number of mobility steps (hops) that a UE can make. For example, if the DU has five cells and you specify a <i>Hops</i> value of 4, the a UE can move from cell1 to cell 2 (first hop), then to cell 3 (second hop), then to cell 4 (third hop), then to cell 5 (fourth hop): each move is a hop.

Test Suite settings


Each Scenario Group will have one or more Test Suites, each of which defines a set of procedures that will be sequentially executed during a test run.



You define one or more Test Suites for each of the Scenario Groups that you define for a test.

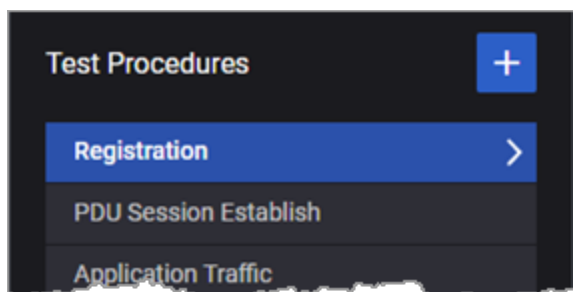
From a selected Scenario Group's **Test Suites** list, click an entry to open its **Test Suite** properties panel.

The following table describes the configuration settings in the **Test Suite** properties panel.

Setting	Description
	Select the Delete Test Suite icon to delete this Test Suite from the selected Scenario Group.
Call Attempt/s	<p>The number of Registration procedures (the first procedure in the call flow) to attempt per second.</p> <p>For example, if you set value to 100 and your Subscriber range has 1000 UEs, then it will take 10 seconds to complete all of the UE registration attempts.</p> <p>The <i>Call Attempt/s</i> value should not be greater than the subscriber range's <i>Range Count</i> value.</p>
Loop Enabled	<p>Select <i>Loop Enabled</i> if you want the call flow to loop continuously throughout the test execution.</p> <p>When you select this option, DuSIM ignores the <i>Repetition</i> setting.</p>
Repetition	<p>The number of times that the test will repeat the complete list of procedures defined in the Test Procedures call flow.</p> <p>The <i>Repetition</i> and <i>Repetition Delay</i> settings are ignored if the <i>Loop Enabled</i> setting is selected.</p>
Repetition Delay (ms)	<p>Specifies a delay (in milliseconds) between successive executions of the test procedures defined under this Test Suite.</p> <p>For example, if you set <i>Repetition</i> to 7 and the <i>Repetition Delay</i> to 1000, then the call flow will run seven times with a one second delay between successive repetitions.</p>
Test Procedures	<p><i>Test Procedures</i> defines a procedural call flow: a set of procedures that are executed in the order listed. During test execution, DuSIM calls each procedure in turn.</p> <p>Refer to Test procedures for SA on the facing page, Test procedures for NSA tests on page 184, and Test procedures for SA and NSA on page 198 for detailed information.</p>

Test procedures for SA

Each Test Suite requires the definition of a procedural call flow, which is an ordered set of procedures that are executed when the test is run. The specific procedures that are available depend upon whether the test is configured for SA testing or NSA testing. The procedures listed below are available only for SA tests.



Note that SA tests can also use the procedures listed in [Test procedures for SA and NSA on page 198](#).

Procedure descriptions:


Deregistration	177
PDU Session Establish	178
PDU Session Release	180
Registration	182
Service Request	183

Deregistration

This test procedure allows the simulated UEs to deregister from the network, in compliance with the 5GMM Deregistration procedure defined in 3GPP TS 24 501, paragraph 5.5.2. The Deregistration procedure is used by a UE to inform the network that it no longer needs access to the 5G system; and it is used by the network to inform the UE that it no longer has access to the 5G system.

Deregistration is the recommended last procedure in a defined DuSIM Test Suite **Test Procedures** call flow.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Deregistration
<i>Properties:</i>	
Deregistration at Power-Off	Select this option to indicate that the Deregistration Request type is set to "Switch Off".

PDU Session Establish

This test procedure complies with the 5GSM PDU session establishment procedure defined in 3GPP TS 24.501, paragraph 6.4.1. The PDU Session Establish procedure can be triggered by a UE or by the network. When initiated by a UE it is used in various circumstances, including establishment of a new PDU session, switching an existing PDU session between non-3GPP access and 3GPP access, and requesting a session for emergency services. Its presence is optional in all Test Suite **Test Procedures** call flows.

Configuration settings


Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select PDU Session Establish
<i>General:</i>	
Instance	The identifier of this PDU Session between a UE and the 5G network.
Abort Session on Error	Enable or disable the Abort Session on Error option for this session. <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>Access Point Name:</i>	
Access Point Name	The Access Point Name (APN) with which the UEs executing this procedure are associated.

Setting	Description
<i>NR Parameters:</i>	
PDU Session ID	The identifier of this PDU Session between a UE and the 5G network.
<i>Parameters:</i>	
Request Type	The request type PDU session establishment: <ul style="list-style-type: none"> Initial Request: establish a new PDU Session. Emergency: establish an emergency session with an Emergency APN.
PDU Type	The Packet Data Unit (PDU) type to use for the PDU session. The available options are IPv4, IPv6, and IPv4v6. When IPv4v6 is selected, the UEs can acquire an IPv4 and an IPv6 IP address. The UEs will be able to run IPv4 and IPv6 traffic (simultaneous or separately).
NRSM Info Transfer Flag	This options specifies: <ul style="list-style-type: none"> if the ESM information transfer flag IE is included in the PDN CONNECTIVITY REQUEST message if ESM information, i.e. protocol configuration options or APN or both, is to be transferred security protected. <p>The ESM information transfer flag IE is described in 3GPP TS 24.301, subclause 9.9.4.5.</p> <p>It is possible to select one of the following values:</p> <ul style="list-style-type: none"> Disabled: the ESM information transfer flag IE is included but the security protected ESM information transfer is not required Enabled: the ESM information transfer flag IE is included and the security protected ESM information transfer is required Not included: no ESM information transfer flag IE is included in the PDN CONNECTIVITY REQUEST message.
PDU Session ID	The identifier of this PDU Session between a UE and the 5G network.
S-NSSAI	The S-NSSAIs (Single Network Slice Selection Assistance Information) information element for this PDU session.
APN	The Access Point Name (APN) on which to establish a Packet Data Network (PDN) connection. This parameter identifies the PDN to which the UEs in the range are requesting connection.
PCO	This parameter specifies the list of protocol configuration options in hexadecimal format, as defined in 3GPP TS 24.008, table 10.5.154. Refer to 3GPP TS 24.008 subclause 10.5.6.3 for further information about the Protocol Configuration Options IE.

PDU Session Release

The PDU Session Release test procedure allows the UE to request the release of a PDU session, in compliance with the 5GSM PDU session release procedure defined in 3GPP TS 24.501, paragraph 6.4.3.

Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select PDU Session Release
<i>General:</i>	
Instance	Enter a value for this instance of the procedure.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>Access Point Name:</i>	
Access Point Name	The Access Point Name (APN) with which the UEs executing this procedure are associated.
<i>NR Parameters:</i>	


Setting	Description
PDU Session ID	The identifier of this PDU Session between a UE and the 5G network.
<i>Parameters:</i>	
PDU Session ID	The identifier of this PDU Session between a UE and the 5G network.
PCO	This parameter specifies the list of protocol configuration options in hexadecimal format, as defined in 3GPP TS 24.008, table 10.5.154. Refer to 3GPP TS 24.008 subclause 10.5.6.3 for further information about the Protocol Configuration Options IE.

Registration

This test procedure allows the simulated subscriber to register and attach to the network, in compliance with the 5GMM Registration procedure defined in 3GPP TS 24.501, paragraph 5.5.1. A UE initiates the registration procedure with a network to obtain authorization to receive services, enable mobility tracking, and enable reachability. The Registration procedure is used when the UE needs to perform Initial Registration to the 5G system, Mobility Registration Update, or Periodic Registration Update.

Registration is always the first procedure in a defined DuSIM Test Suite **Test Procedures** in SA mode.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Registration.

Service Request

This test procedure allows the simulated UEs to send the SERVICE REQUEST message to the AMF, in compliance with the Service request procedure defined in 3GPP TS 24.501, paragraph 8.2.16. The Service Request procedure can be triggered by a UE or by the network. It is used by a UE in CM-IDLE state or by the 5GC to request the establishment of a secure connection to an AMF (Access and Mobility Function). The procedure is also used both when the UE is in CM-IDLE and in CMCONNECTED to activate a User Plane connection for an established PDU Session. Its presence is optional in all Test Suite **Test Procedures** call flows.

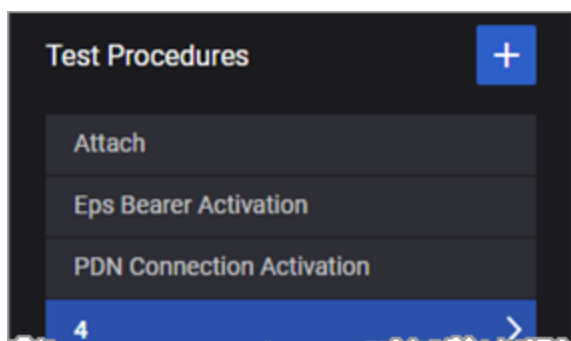
Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Service Request
<i>General:</i>	
Instance	Please contact Technical Support for assistance with this option.
Abort Session on Error	Enable or disable the Abort Session on Error option for this session. <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>EmergencyServicesFallback mode:</i>	
Service Type	Select the service type: <ul style="list-style-type: none"> data: The UE in CM-IDLE state initiates the Service Request procedure in order to send user data.

Setting	Description
	<ul style="list-style-type: none"> emergency services: The UE sends the Service Request message indicating that it requires emergency services. emergency services fallback: The UE sends the Service Request message indicating that it requires emergency services fallback. high priority access: The UE sends the Service Request message indicating that it requires high priority access.

Test procedures for NSA tests

Each Test Suite requires the definition of a procedural call flow, which is an ordered set of procedures that are executed when the test is run. The specific procedures that are available depend upon whether the test is configured for SA testing or NSA testing. The procedures listed below are available only for NSA tests



Note that NSA tests can also use the procedures listed in [Test procedures for SA and NSA on page 198](#).


Procedure descriptions:

Attach	185
Detach	186
ENDC Configuration Update	187
EPS Bearer Activation	188
EPS Bearer Deactivation	189
Inter eNB Handover	190
PDN Connection Activation	191
PDN Connection Deactivation	193
SCG Release	195
SGNB Addition	196

Attach

The simulated UEs use the Attach procedure to establish connection with the LTE network in NSA mode. Attach is always the first procedure in a defined DuSIM Test Suite(NSA mode).


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Attach.
<i>Properties:</i>	
Instance	The identifier of this PDU Session between a UE and the 5G network.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.

Detach

This test procedure allows the simulated UEs to detach from the LTE network. Detach is the recommended last procedure in a defined DuSIM Test Suite Test Procedures call flow in NSA mode.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Detach
<i>Properties:</i>	
Instance	The identifier of this PDU Session between a UE and the 5G network.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.

ENDC Configuration Update

ENDC (E-UTRAN New Radio – Dual Connectivity) is an NSA procedure that allows mobile devices to simultaneously access 5G and 4G networks. It was introduced in 3GPP release 15.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (muti-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select ENDC.
<i>Properties:</i>	
Cell Assistance Information	Enable this option to use the Cell Assistance Information IE to generate the List of Served NR Cells IE and include the list in the EN-DC CONFIGURATION UPDATE ACKNOWLEDGE message.
Served E-UTRA cells to modify	The list of modified cells served by the eNB.
Served E-UTRA cells to delete	The list of deleted cells served by the eNB.

EPS Bearer Activation

The EPS Bearer Activation procedure is performed when a UE attaches to the network.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select EPS Bearer Activation
<i>General parameters:</i>	
Instance	The identifier of this PDU Session between a UE and the 4G network.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>LTE Bearer:</i>	
Bearer Type	Select the desired LTE Bearer Type from the drop-down list.
<i>Access Point:</i>	
Access Point Name	The Access Point Name (APN) on which to establish a Packet Data Network (PDN) connection. This parameter identifies the PDN to which the UEs in the range are requesting connection.

EPS Bearer Deactivation

The EPS Bearer Deactivation procedure is used to deactivate a dedicated bearer or deactivate all bearers belonging to a PDN address. This DuSIM procedure is used to deactivate a specific type of LTE bearer that has been established earlier in the call flow..


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select EPS Bearer Activation
<i>General parameters:</i>	
Instance	The identifier of this PDU Session between a UE and the 4G network.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>LTE Bearer:</i>	
Bearer Type	Select (from the drop-down list) the desired LTE Bearer type that will be deactivated.

Inter eNB Handover

This test procedure initiates an Inter-eNodeB Handover procedure, as described in TS 36.331, for NSA testing. This procedure is executed when a UE moves from an eNodeB cell to a cell controlled by a neighboring eNodeB.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Inter eNB Handover
<i>Inter eNB Handover Parameters:</i>	
EPS Bearer ID 5 through ID 15	Activate the EPS bearers supported by the mobile equipment; at least one of the available EPS Bearer IDs must be selected.
gNB Target LSU Cell ID	The gNodeB target Cell ID.
SCG Changed	Enable this option if an Secondary Cell Group (SCG) is configured and the SCG changes during the handover (as in the case of dual connectivity).
Target SCG Cell ID	The Cell ID of the handover target Secondary Cell Group (SCG).

PDN Connection Activation

This procedure is used for NSA tests. The PDN connectivity procedure is used by the UE to request the setup of a default EPS bearer to a PDN.

Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select PDN Connection Activation
<i>General:</i>	
Instance	The identifier of this PDU Session between a UE and the network.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>Access Point Name:</i>	
Access Point Name	The Access Point Name (APN) with which the UEs executing this procedure are associated.
<i>PDN Parameters:</i>	
Request	The request type PDU session establishment:


Setting	Description
Type	<ul style="list-style-type: none"> • Initial Request: establish a new PDU Session. • Handover: initiate a handover. • Emergency: establish an emergency session with an Emergency APN.
PDN Type	Select the desired PDN type: IPv4, IPv6, or IPv4v6.
ESM Info Transfer Flag	Select this option to include the ESM information transfer flag IE. It indicates whether ESM information (protocol configuration options or APN, or both) is available for retrieval by the network.
PCO	This parameter specifies the list of protocol configuration options in hexadecimal format, as defined in 3GPP TS 24.008, table 10.5.154. Refer to 3GPP TS 24.008 subclause 10.5.6.3 for further information about the Protocol Configuration Options IE.

PDN Connection Deactivation

This test procedure allows to deactivate the specified PDN connection for NSA mode.

This procedure is used for NSA tests. It is used by the UE to request deactivation of a specified PDN connection.

Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select PDN Connection Deactivation
<i>General:</i>	
Instance	The identifier of this PDU Session between a UE and the network.
Abort Session on Error	Enable or disable the Abort Session on Error option for this session. <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>Access Point Name:</i>	
Access Point Name	The Access Point Name (APN) with which the UEs executing this procedure are associated.
<i>PDN Parameters:</i>	

Setting	Description
PCO	This parameter specifies the list of protocol configuration options in hexadecimal format, as defined in 3GPP TS 24.008, table 10.5.154. Refer to 3GPP TS 24.008 subclause 10.5.6.3 for further information about the Protocol Configuration Options IE.


SCG Release

This test procedure allows to trigger Secondary 5G gNB node release. Its presence is optional in all Test Suite Test Procedures call flows.

SGNB Addition

This procedure initiates a 5G Secondary gNB (SgNB) Addition procedure, as defined in 3GPP TS 36.423.

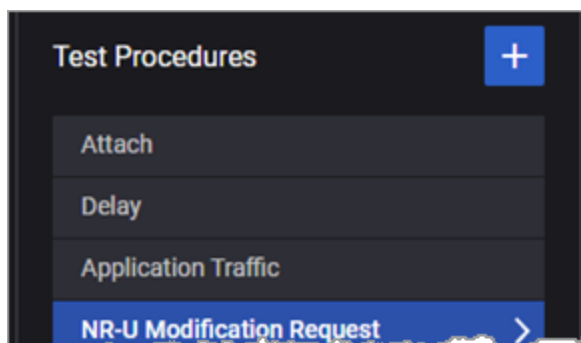
Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	<p>Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures.</p> <p>Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.</p>
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select SGNB Addition
<i>General Parameters:</i>	
Instance	The identifier of this PDU Session between a UE and the 5G network.
Abort Session on Error	<p>Enable or disable the Abort Session on Error option for this session.</p> <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
<i>SGNB Addition Parameters:</i>	
gNB Target LSU Cell ID	The gNodeB target Cell ID.
EPS Bearer ID 5 through ID 15	Activate the EPS bearers supported by the mobile equipment; at least one of the available EPS Bearer IDs must be selected.

Setting	Description
Extensions	Select the desired extensions (or None) from the drop-down list. Each extension (except None) provides a set of associated parameters.

Test procedures for SA and NSA

Each Test Suite requires the definition of a procedural call flow, which is an ordered set of procedures that are executed when the test is run. The specific procedures that are available depend upon whether the test is configured for SA testing or NSA testing. The procedures listed below are available for SA and NSA tests.




Procedure descriptions:

Application Traffic	199
Delay	200
DU Initiated Release	201
NR-U Modification Request	202

Application Traffic

The Application Traffic procedure generates user plane traffic; the specific traffic that is generated is determined by the UE Test Objective settings. The presence of this procedure is optional in all Test Suite **Test Procedures** call flows.


Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Application Traffic
<i>NR Parameters:</i>	
PDU Session ID	The identifier of this PDU Session between a UE and the 5G network.
<i>Application Traffic Parameters:</i>	
Duration (s)	The number of seconds during which the application traffic flow will be active.

Delay

The purpose of the Delay procedure is create a delay between successive procedures in the call flow. Its presence is optional in all Test Suite **Test Procedures** call flows.

Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select Delay.
<i>Properties:</i>	
Instance	The identifier of this PDU Session between a UE and the 5G network.
Abort Session on Error	Enable or disable the Abort Session on Error option for this session. <ul style="list-style-type: none"> When this option is enabled, the test session aborts if this test procedure fails; if a Detach is scheduled in any subsequent test procedure, the Detach is executed before aborting the test session. When this option is not enabled, the test session continues to execute the following test procedures, although the current test procedure fails.
Success Percentage Threshold	This parameter specifies the threshold at which the execution result of the test procedure becomes successful. It is the percentage ratio of the number of successful executions to the number of total executions.
Delay time (ms)	The number of milliseconds to wait before starting the next procedure in the procedure list.


DU Initiated Release

This test procedure allows the simulated UEs to trigger a gNB-DU initiated UE Context Release Request as defined in 3GPP TS 38.472 section 8.3.2 towards the gNB-CU. It is used by a UE to move into CM IDLE state. Its presence is optional in all Test Suite Test Procedures call flows.

NR-U Modification Request

The simulated UEs use the NR-U Modification Request to modify NR user plane protocol values that the DU sends to the CU, via the DL Data Delivery Status PDU. Refer to TS 38.425 for detailed information about the NR user plane protocol.

Configuration settings

Setting	Description
	Select the Delete Procedure icon to delete this procedure from the call flow.
<i>Defining Parallel procedures:</i>	
Parallel Procedure	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, DuSIM changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 40 for instructions for configuring parallel procedures.
Repetition	Enter the number of times that the parallel procedure will execute for this step in the call flow.
<i>Procedure selection:</i>	
Procedure Type	Select NR-U Modification Request.
<i>NR-U Modification Request Parameters:</i>	
DRB ID	The data radio bearer identifier. Each NR user plane protocol instance is associated to one data radio bearer only, which is identified by the DRB ID. There is one NR user plane instance per GTP tunnel.
DU ID	The DU ID uniquely identifies the gNB-DU within a gNB-CU.
Trigger Type	Select the type of trigger from the drop-down list: <ul style="list-style-type: none"> Triggered DDDS: triggers the Downlink Data Delivery Status procedure. Trigger Assisted Information: triggers the Transfer of Assistance Information procedure. The Trigger Type determines which values are delivered from the DU to the CU.
<i>Triggered DDDS Parameters:</i>	
Radio Linkage Outage	Select the desired value from the drop-down list: these values are encoded in the Cause Value field. This parameter sets an indication of detected radio link outage or radio link resume for the data radio bearer.
Final Frame Indication	Enable this option to set the Final Frame Indication bit in the DL Data Delivery Status PDU.

Setting	Description
Desired Data Rate (bytes/sec)	Enter the amount of data desired to be received (in bytes) in a specific amount of time (1 second) for the data radio bearer established for the UE. This value is used for flow control.
Desired Buffer Size (bytes/sec)	Enter the desired buffer size (in bytes) for the data radio bearer. This value is used for flow control.
<i>Trigger Assistance Information Parameters:</i>	
PDCP Duplication Activation Suggestion	Use this option to activate or inactivate the PDCP Duplication Activation Suggestion, which informs the CU of the suggestion from the DU on whether or not to activate DL PDCP duplication.
Assisted Information type	Select the desired type of radio quality assistance information from the drop-down list. The types include: Unknown, Average CQI, Average HARQ Failure, Average HARQ Retransmissions, DL Radio Quality Index, UL Radio Quality Index, Power Headroom Report, and some reserved values.
Radio Quality Assistance Information	This parameter indicates one of the assistance information indicated by the Assistance Information Type. The value range is zero through 255, where zero represents the lowest quality.

CHAPTER 17

Manage and use test sessions

When you create a new test, DuSIM establishes a *test session* which remains available until such time as you decide to delete it (if ever). This way, you can access existing test configurations to change the settings and to view details, or to re-run a test session.

Chapter contents:

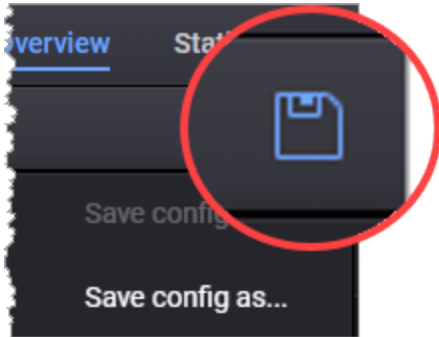
Save test sessions	205
Manage test sessions	206
Import and export sessions	210
Delete configs and sessions	212

Save test sessions

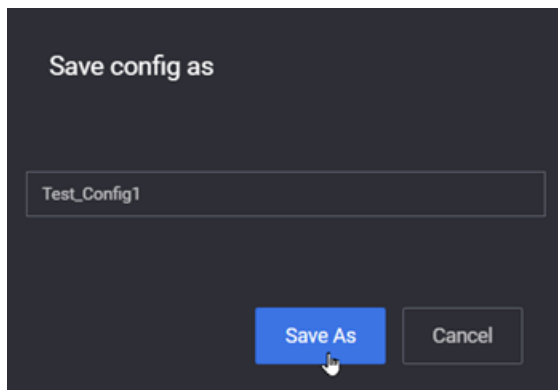
Once a test is configured (for details, refer to [Create a new test config on page 19](#)), you can record its configuration as a session, edit and save it for future use.

To save a configuration file, do the following:

1. Click the **Save** icon from the upper-right corner of the **Test Overview** page.

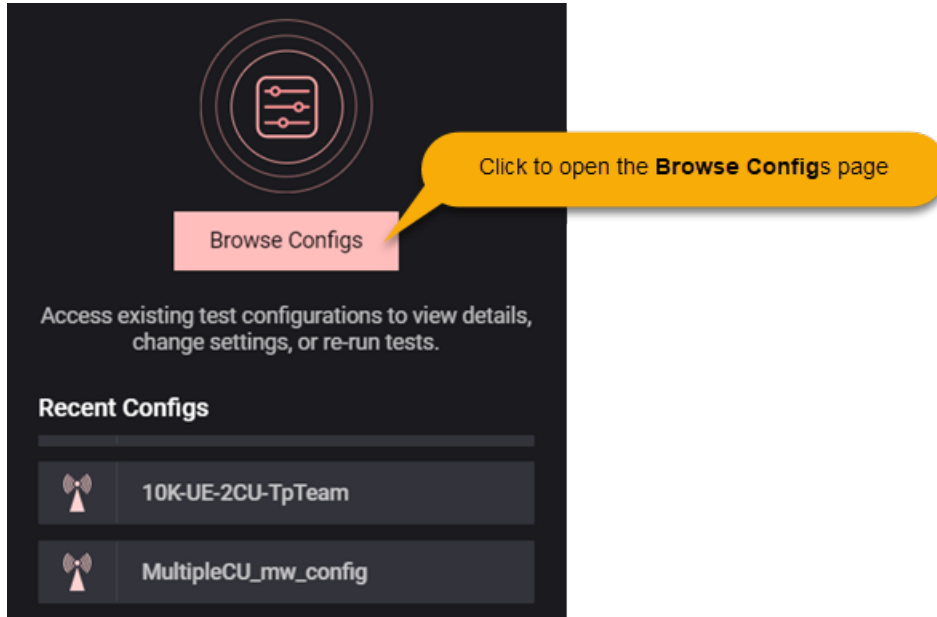


2. Choose one of the following:
 - a. Either **Save config** to quickly save your test configuration.
 - b. Or, **Save config as** to save your test configuration with a specific name; then enter a name for the test configuration and click the **Save as** button.



Manage test sessions

Managing saved tests is done on the **Browse Configs** page. To access the page, click the **Browse Configs** button from the main DuSIM Dashboard.



The **Recent Configs** list contains default configurations plus previously loaded configurations. If you select one of the configurations (by clicking it) a new session is created with this configuration loaded inside of it.

NOTE

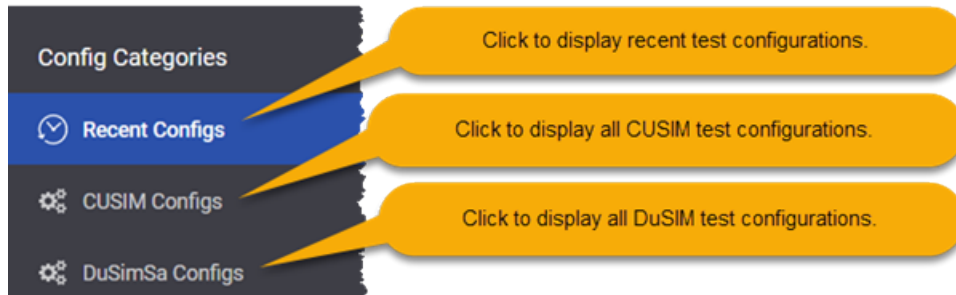
If the selected configuration is already opened in an existing session, a message is displayed allowing you to open that session or to create a new session based on the selected test configuration.

The **Browse Configs** page is split into two main sections, each one having a specific role in handling your tests configurations:

- [View configuration categories on the next page](#)
- [Manage configurations on the next page](#)

View configuration categories

The **Config Categories** area allows you to switch between displaying your recent test configurations or displaying them based on their category.



NOTE

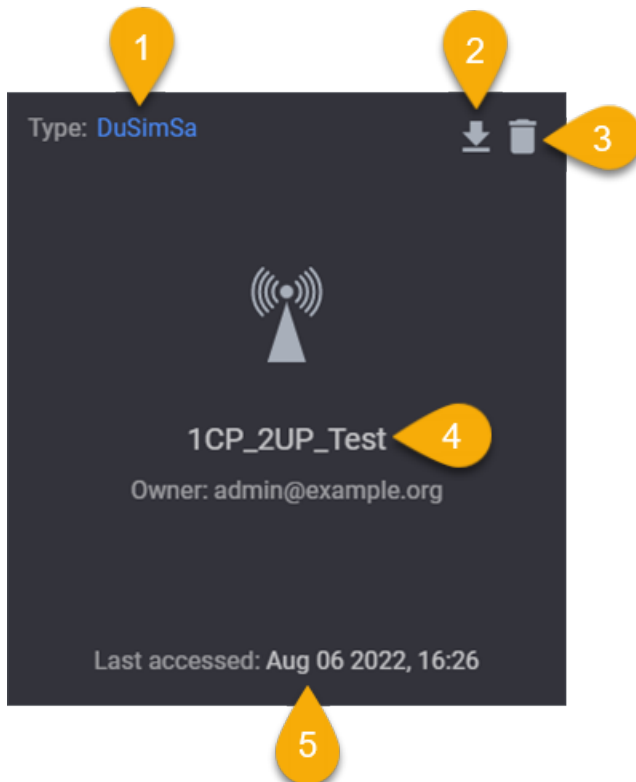
The **Recent Configs** category displays only the last twenty configurations in chronological order, the first being the most recent from all the categories listed above. In order to see all of your tests, you can display them sorted by category, by selecting a specific test category under **Recent Configs**.

Manage configurations

On this section, DuSIM displays your test configurations suite, offering you details on the specific test configuration and allowing you to delete it or to export it.

For each test category, test configurations can be displayed as tiles or rows.



A test configuration displayed as a tile

1	Indicates the test type
2	Click the button to export the test configuration
3	Click the button to delete the test configuration
4	Details on the test name and test owner
5	Timestamp of the last test session

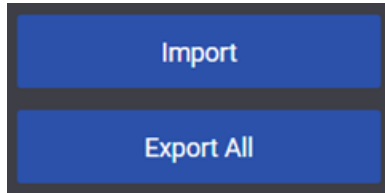
Test configurations displayed as rows

	1	2	3	4	5
	Config Name	Last accessed	Application	Config Type	Owner
6	<input type="checkbox"/> SC_50Cell_UE4000	Aug 23, 2022, 1:26:22 PM		DuSimSa	admin@example.org
7	<input checked="" type="checkbox"/> DuSIM Standalone Base Config	Aug 23, 2022, 12:20:34 PM		DuSimSa	system
	<input type="checkbox"/> Chanchal_MultiCell_test_3	Aug 22, 2022, 10:35:32 AM		DuSimSa	admin@example.org
	<input type="checkbox"/> 10K-UE-2CU-TpTeam	Aug 11, 2022, 9:56:37 PM		DuSimSa	admin@example.org
	<input type="checkbox"/> MultipleCU_mw_config	Aug 7, 2022, 7:18:20 AM		DuSimSa	admin@example.org
	<input type="checkbox"/> 1CP_2UP_Test	Aug 6, 2022, 4:26:49 PM		DuSimSa	admin@example.org
8	Delete	Export	9		

1	Details on the test name
2	Timestamp of the last test session
3	Indicates the test type
4	Indicates the test owner
5	Click the button to create a session based on the configuration
6	Use to select a test configuration
7	Indicates a base configuration <div>NOTE For the base configurations, the test owner is <i>system</i>.</div>
8	Click the button to delete the test configuration
9	Click the button to export the test configuration

Import and export sessions

You can import and export test configurations by clicking the **Import** or **Export all** buttons which are found on the **Config Categories** area of the **Browse Configs** page.

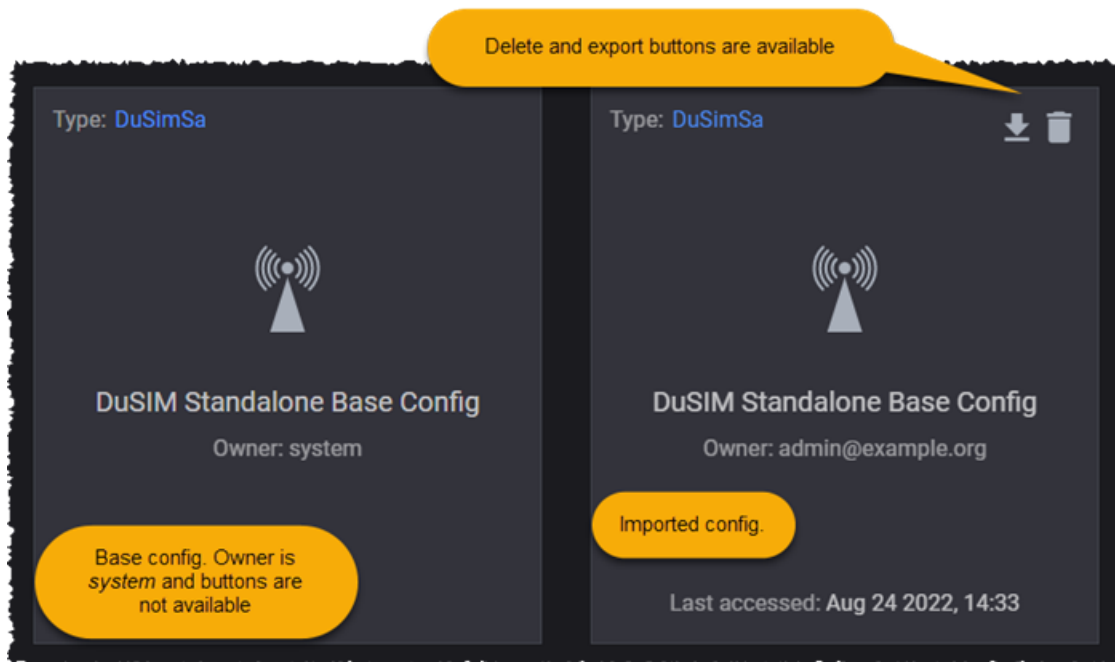


Import test configurations

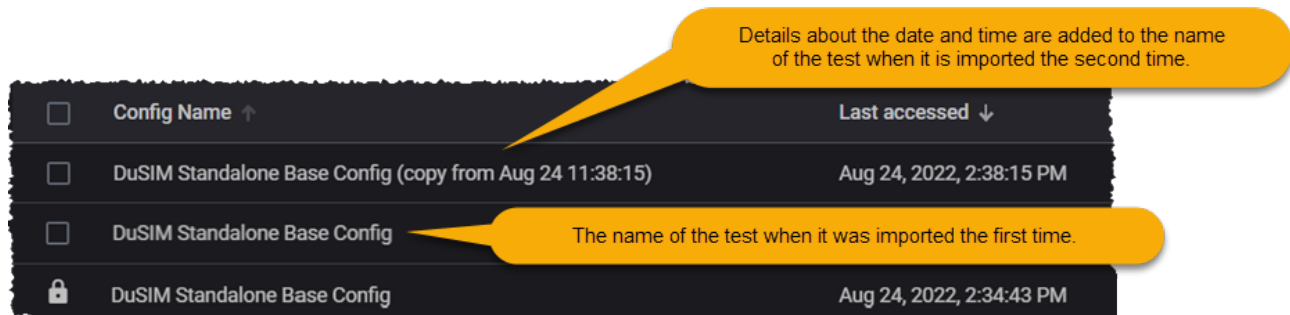
To import a saved test configuration from disk, do the following:

1. From the **Dashboard** page, click the **Browse Configs** button. The **Browse Configs** page appears.
2. From the **Test Categories** section, click the **Import** button.
3. Select the test configuration you want to import from the ones available at your download location.
4. Click **Open** to add the test configuration to the dashboard.

Imported tests can have any name, even the name of the base configuration tests. You can differentiate between a base configuration test and an imported test by the icons on the top-right corner of the test tile. The imported test is a user test that has the delete and export buttons on the top-right corner of the test tile. Also, each test will display the name of the test owner.



If a test is imported twice with the same name, the second time the test name will be displayed with details about the date and time of the import.



The screenshot shows a table with two columns: 'Config Name' and 'Last accessed'. It lists three configurations. Two callouts explain the naming: one points to the second row's name, stating that date and time details are added upon second import; the other points to the third row's name, stating it is the name from the first import.

Config Name ↑	Last accessed ↓
DuSIM Standalone Base Config (copy from Aug 24 11:38:15)	Aug 24, 2022, 2:38:15 PM
DuSIM Standalone Base Config	
DuSIM Standalone Base Config	Aug 24, 2022, 2:34:43 PM

NOTE

By default, when you import a new test, the displayed name is the name you have in the JSON file under `displayName` - in this case, the `displayName` is DuSIM Standalone Base Config. The second time it is imported, the test name is concatenated with *Imported* <date> <time>.

Export a saved test configuration

To export a saved configuration, do the following:

1. From the **Dashboard** page, click the **Browse Configs** button. The **Browse Configs** page appears.
2. From the **Test Categories** section, select the category containing the test to be downloaded.
3. Select the test configuration you want to download and click the **Export** button. When in tile view mode, click the **Download** button from the test tile.
4. Specify the download file name and select the download location.
5. Click **OK** to download the test configuration.

NOTE

The configuration file is exported as a JSON file.

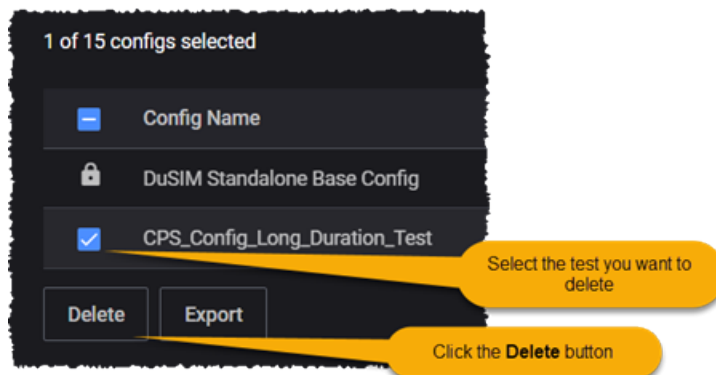
Delete configs and sessions

The terms *test config* and *test session* are not entirely synonymous. A "config" refers to a configuration definition file (JSON format), whereas a "session" is an instance of that file that is loaded in memory and is capable of being run.

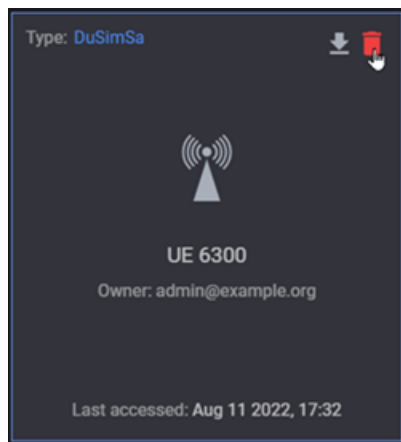
How to delete a DuSIM config

To delete a saved configuration from the **Browse Configs** page, do the following:

1. From the **Dashboard** page, click the **Browse Configs** button. The **Browse Configs** page appears.
2. From the **Test Categories** section, select the category containing the test to be deleted.
3. Select the test configuration you want to delete and click the **Delete** button.



When in tile view mode, click the **Delete** button from the test tile .



This will delete the configuration from the database, but not the session itself.

Important notes

Before deleting a session, be aware of the following application behaviors:

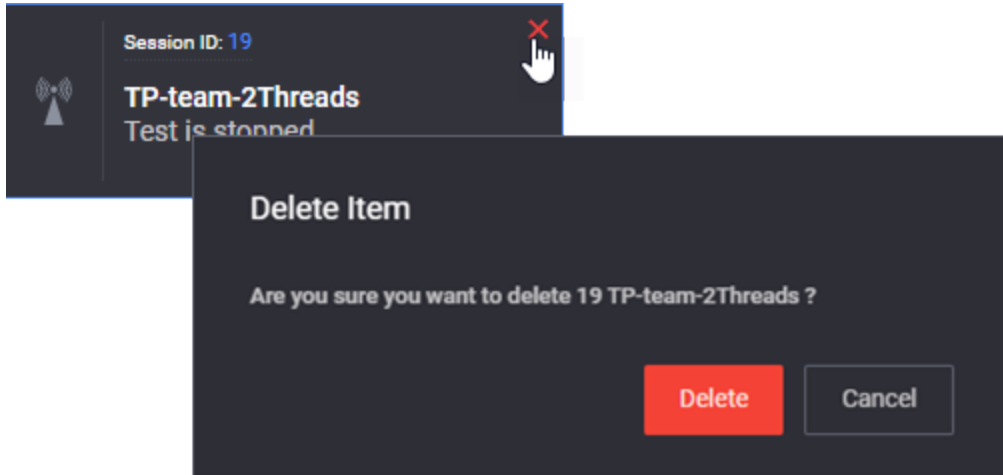
- The session will be permanently removed and cannot be recovered.
- However, when you delete a session, the session's config is not deleted. Therefore, you can create new sessions based on that config.

- If you have a session open, and you delete the config upon which the session is based, the session is not deleted. Therefore, you can open the session and save a new config from it.

How to delete a Keysight Open RAN Simulators, Cloud Edition 3.0 session

You can also delete a test session from the Dashboard:

1. Go to the **Dashboard**. (Click the Keysight logo from any point in the interface to return to the dashboard page.)
2. Locate the tile for the session that you plan to delete, then click the **X** in the upper right corner. Keysight Open RAN Simulators, Cloud Edition 3.0 opens a confirmation dialog.



3. Select **Delete** to confirm the action.

CHAPTER 18

Manage DuSIM licenses

DuSIM is a licensed product. You can manage licenses using either the integrated DuSIM License Manager or a centralized License server that is managed by your organization.

Chapter contents:

Licensing Requirements	215
License Manager	216
License server	218

Licensing Requirements

The license server is shipped as a separate `.ova` file.

After deploying the `.ova`, you will have access to a web interface for the license server (for example: <https://10.38.156.169>) .

You can:

- activate licenses by selecting the **Activate** button,
- sync licenses,
- generating a license request bin file by selecting **Offline Operations** and then **Generate Request**,
- import offline licenses by selecting **Offline Operations** and then **Import Licenses**,
- check the license statistics,
- deactivate Licenses by selecting the **Deactivate** button.

After activation, the licenses and features will be available in the DuSIM web UI.

License Manager

The first time you use DuSIM, you need to active at least one license. You activate and manage your licenses using the DuSIM **License Manager** functions, which are accessed from the setup menu.

- [How to open License Manager below](#)
- [Activate a license below](#)
- [Deactivate a license below](#)
- [Sync licenses below](#)
- [Reserve a license on the next page](#)
- [Get license statistics on the next page](#)
- [Perform offline license operations on the next page](#)

How to open License Manager

To access the DuSIM License Manager:

1. Select **Administration** from the setup menu (⚙️).
2. Select **License Manager** (from the **Adminstration** menu).

Activate a license

To activate one or more DuSIM licenses:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select **Activate licenses**.
DuSIM opens the **Activate Licenses** dialog.
3. Enter your license data in the dialog box.
You can use either activation codes or entitlement codes (one or more).
4. Select **Load Data**, indicate the number of licenses you want to activate, then click **Activate**.

Your new licenses—which should now be listed in the License Manager page—are now available for running tests.

Deactivate a license

To activate one or more DuSIM licenses:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select **Deactivate licenses**, then and indicate a new quantity for each of the existing licenses.
3. Select **Perform the Activation** to complete the task.

Sync licenses

To synchronize one or more DuSIM licenses:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select **Sync licenses**.

Reserve a license

To reserve one or more DuSIM licenses:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select the **Manage Reservation** icon.
DuSIM opens a new window.
3. Select the license you wish to reserve.
4. Enter the number of desired licenses in **New Reserved Count** field.
5. Enter the duration of the reservation (in hours) in the **Duration to Reserve** field.

NOTE

The License Statistics display shows all reserved features, ordered by count and reserved time. The initial reserved count and duration is overwritten when a new reservation is performed.

Get license statistics

To activate one or more DuSIM licenses:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select **License statistics**.

Perform offline license operations

Offline license management is required for cases in which your test network is operating in an isolated environment with no Internet access. To perform offline DuSIM license operations:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select **Offline operations**.
DuSIM opens the **Keysight Licensing Offline Operations** dialog.
3. Click **Generate request**.
4. Using a system that has Internet connectivity, access the KSM Offline Operations Page, and follow the steps provided for the desired operation.
5. From your offline system, return to the **Keysight Licensing Offline Operations** dialog, then click **Import license**.
6. Click **Finish** to complete the task.

License server

Rather than using the internal DuSIM License Manager, you can use a centralized License server that is managed by your organization.

Add a License Server

To add a license server in the DuSIM web UI:

1. Log in the DuSIM web UI.
2. Under the Settings Menu (⚙️), select License Servers.

The dialog shows the license server currently used.

NOTE

To see the list of installed licenses, you need to access the license server in a web browser: <https://<license-Server-IP>>

3. Enter the license server IP address in the empty license server field, then select the Add button (+) next to the field.
4. Select **CLOSE** to confirm your action and close the License server dialog.

Remove a License Server

To remove a license server that was previously added in the DuSIM web UI:

1. Log in the DuSIM web UI.
2. Under the Settings menu (⚙️), select License servers.
The license servers dialog opens. listing the previously-set license servers.
3. Select the **Delete** button next to the license server that you want to remove.
4. Select **CLOSE** to confirm your action and close the License server dialog.

Activate a license

To activate one or more DuSIM licenses:

1. From the Setting menu (⚙️), select **Application Settings**.
DuSIM opens the **Applications Settings** dialog.
2. Select a **License Provider** from the drop-down list.
3. Enter the IP address in the **License Server IP** field.
4. Click **Update**.

CHAPTER 19

Manage DuSIM users

Managing the users who can access the application is one of the primary DuSIM administrative requirements.

- [User categories below](#)
- [Creating users below](#)
- [Reset a user's password on the next page](#)
- [Disable a user account on the next page](#)
- [Delete a user account on the next page](#)
- [Additional user management functions on page 221](#)

User categories

DuSIM user accounts can be of one of the following types:

- Administrative user: Can access the Access Control functions and perform various administrative tasks, including the definition and management of other user accounts.
- Regular user: Can access the application and use all of the resources involved in test creation, execution, and analysis.

Creating users

Each user who requires access to the DuSIM application must have a user account. To add a user:

1. Select the settings menu (⚙️) and then select **User Management**.
DuSIM opens the **Keycloak Admin Console** in a new browser tab.
2. Select **Users** from the list of **Manage** functions (in the navigation pane).
3. Select the **Add user** button.
4. Enter the required information in the **Add user** form, then select the **Save** button.
The following values are required for the new user:
 - Username (which must be unique within the realm).
 - Email address
 - First and Last Name
 - *User Enabled* set to **ON**.
5. Select the **Save** button.
DuSIM adds the user and displays that user's information in the **Details** tab.
6. Set the initial password for the user:

- a. Select the **Credentials** tab.
- b. Enter the *Password*.
- c. Re-enter the password in the *Password Confirmation* field.
- d. Set *Temporary* **ON** if the user will be required to change the password upon initial log in.
- e. Select the **Set Password** button.
DuSIM displays a confirmation dialog.
- f. Select the **Set Password** button to confirm the action.

Reset a user's password

Administrative users can reset a user's password:

1. Select the settings menu (⚙️) and then select **User Management**.
DuSIM opens the **Keycloak Admin Console** in a new browser tab.
2. Select **Users** from the list of **Manage** functions.
3. Select the user.
4. Select the **Credentials** tab.
5. Enter the new *Password*.
6. Re-enter the new password in the *Password Confirmation* field.
7. Set *Temporary* **ON** if the user will be required to change the password upon initial log in.
8. Select the **Reset Password** button.
DuSIM displays a confirmation dialog.
9. Select the **Reset Password** button to confirm the action.

Disable a user account

Administrative users can temporarily disable a user's account:

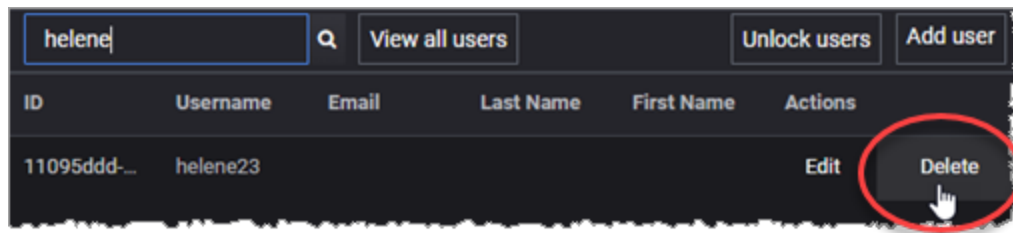
1. Select the settings menu (⚙️) and then select **User Management**.
DuSIM opens the **Keycloak Admin Console** in a new browser tab.
2. Select **Users** from the list of **Manage** functions.
3. Select the user.
4. Set *User Enabled* to **OFF**.

This user account will not be able to log in until the account access is set to **ON**.

Delete a user account

Administrative users can reset a user's password:

1. Select the settings menu (⚙️) and then select **User Management**.
DuSIM opens the **Keycloak Admin Console** in a new browser tab.
2. Select **Users** from the list of **Manage** functions.
3. View all users or search for the Username of the account that you will delete.
4. Click **Delete**.



5. DuSIM opens a confirmation dialog.
6. Select **Delete** to confirm that you are permanently deleting this user account.

Additional user management functions

Additional user management functions are available, in addition to those described in the procedures described above. Most of the functions provide a tool tip that describes its function and usage. For more information about the **Access Control** options and configuration, refer to the official [Keycloak documentation](#).

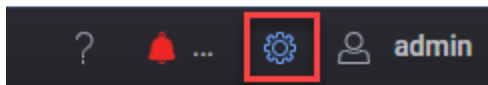
CHAPTER 20


DuSIM title bar settings


The Open RAN Simulators Cloud Edition title bar provides access to a number of important application, system, and user settings. Each of these is described below.

- [Application and system settings below](#)
- [Current user settings on page 224](#)
- [Events notifications on page 224](#)
- [Technical Support and Application Help on page 224](#)

Application and system settings



-  The gear icon opens the Settings menu, which provides access to a number of application and system settings, administrative functions, and application resources:

Setting	Description
License Manager	Select this option to open the License Manager on page 216 window.
Agent Management	Select this option to open the Agent management on page 62 window.
Resource Library	The location to which you can import, and from which you can access, your various application resources, including: packet captures, CA certificates, and objects (SIP, HTTP, Media, Flow, and other).
Software Updates	<p>Select this option to open the Software Updates window.</p> <p>To update to a newer version, do the following:</p> <ol style="list-style-type: none"> 1. Open the Settings menu () and click on Software Updates. 2. Click Select Packages For Upload and open the folder containing the upgrade file. 3. Select the upgrade file and click Open. 4. Click Start Update to initiate the update process. 5. If needed, you can remove the update packages from the update section by clicking Reset Current Changes.

Setting	Description
Application Settings	<p>You use the Application Settings to select the type of License Provider that you are using and to set the License Server IP address. The following options are available for License Provider:</p> <ul style="list-style-type: none"> • External License Server - select this option to set an external license server. • Embedded License Server - the license server that is included in DuSIM MW. <p>Refer to License Manager on page 216 for information about activating and managing licenses.</p>
Logs Level	<p>You use the Logs Level setting to view and change the log level that it set for the DuSIM Controller. The logs level determines the type of data that are written to the log files:</p> <ul style="list-style-type: none"> • Error: Designates messages indicating that an error has occurred that impacts application stability. • Warn: Designates messages indicating that an error has occurred that potentially impacts application stability. • Info: Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug: Designates fine-grained informational events that are most useful for debugging the application.
Data Migration	<p>Allows you to export selected data (such as authentication data and configs) and to import controller data from a migrate package.</p>
System Monitor	<p>The ORAN SIM CE System Monitor provides tools for monitoring and managing the application's system health. There are two such tools:</p> <ul style="list-style-type: none"> • Controller Health: Displays CPU, Memory, and storage utilization data over selectable periods of time. • System Cleanup: Displays the size of the Logs, Diagnostics, and Migration data storage files and permits deletion of any of these.
User Management	<p>Application Administrators use the User Management settings for all aspects of user management. For detailed information, refer to Manage DuSIM users on page 219.</p>

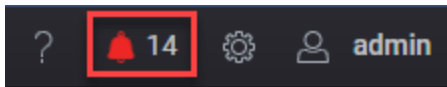
Current user settings



The current user settings provide access to the following functions:

- **User Profile:** Opens the Keycloak Account Management page for the current user. This page enables modification of various user settings, including email address, first and last names, among others.
- **Preferences:** Allows you to switch between the two display themes: light mode and dark mode.
- **Log out:** Log out of your current session.

Events notifications



The events icon shows the number of event notifications that have been received, and the color of the icon reflects the nature of the events. For example, if the events list contains any Error events, the icon will be red.

Refer to [View Notifications and Test Events on page 226](#) for more information about events.

Technical Support and Application Help



The ? menu provides access to the following functions:

- **Contents:** Access to the REST API browser, an API Reference guide, and a collection of application user guides.
- **Technical Support:** An option to collect diagnostics information, contact Keysight Technical Support personnel, view and accept the Keysight EULA, access software downloads, and open the About Open RAN Simulators Cloud Edition dialog. Refer to [Collect Diagnostics on page 228](#) for more information about collecting diagnostics data.

CHAPTER 21

Troubleshooting

DuSIM provides a number of tools and methods to help you evaluate, troubleshoot, and correct problems that may arise during test development and execution.

The main debugging tools that DuSIM provides are notification and event management, messages displayed during test execution, test diagnostics data, and log files.

Chapter contents:

View Notifications and Test Events	226
Collect Diagnostics	228

View Notifications and Test Events

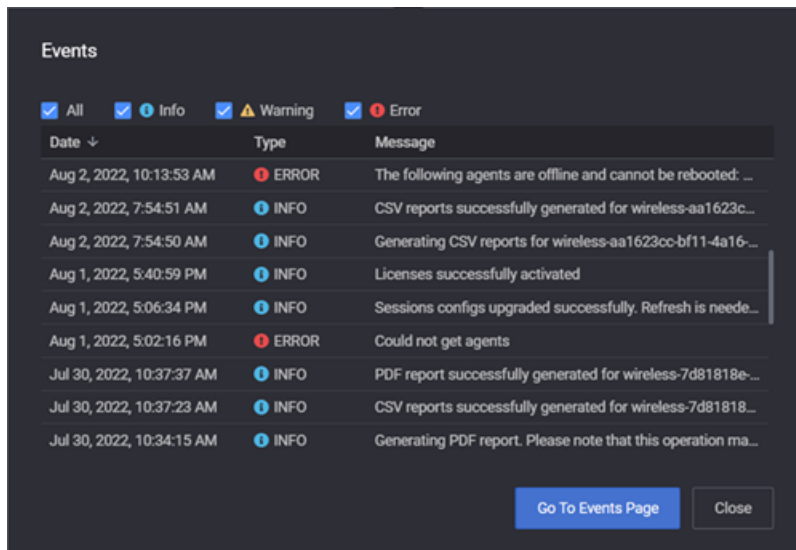
The title bar displays a notifications icon and a counter showing the total number of triggered notifications since the counter was last reset for the current DuSIM instance. The icon and the counter are visible from all the pages of the DuSIM web UI. The notification icon (🔔) indicates in real-time the number of registered events.



The icon is color-coded to reflect the most serious event notification that has been received:

Type		Description
ERROR	<div></div>	An <i>error</i> notification indicates that an error has occurred that impacts application stability. The application is possibly in an unstable or indeterminate state, and the should either be restarted or should carry out error recovery or re-initialization routines.
WARNING	<div></div>	A <i>warning</i> notification indicates an error has occurred that potentially impacts application stability.
INFO	<div></div>	An <i>info</i> notification indicates a general-purpose notification, such as logging data or a heartbeat indicator.

To view more details on the triggered events, select the notifications icon. The **Events** window is displayed.



Here you can view details on the registered events regarding the logging date, their severity type and description. You can choose to display all events or certain types of events, based on their severity, by selecting or clearing the associated check-box.

To view the events page, click the **Go to Events Page** button. Here you can search for events based on the available filtering criteria, like date, message, or event type.

▼ Filter events by

Message	From	To	Notification type
<input type="text" value="Type keywords"/>	<input type="text" value="Select a date"/> ▼	<input type="text" value="Select a date"/> ▼	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Info <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Error

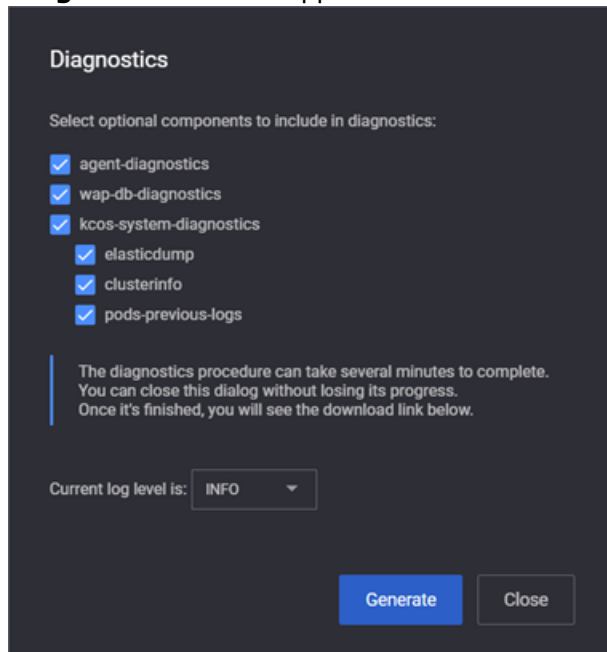
Date ↓	Type	Message
Aug 5, 2022, 7:35:55 PM	ERROR	Low disk space: 8.17%
Aug 5, 2022, 7:06:00 PM	WARNING	Disk space is getting low: 17.35%
Aug 3, 2022, 9:37:10 AM	ERROR	The following agents are offline and cannot be rebooted: 10.36.51.88.
Aug 3, 2022, 9:35:18 AM	ERROR	The following agents are offline and cannot be rebooted: 10.36.51.88.
Aug 2, 2022, 7:24:54 PM	ERROR	Could not upload files for agent 10.36.51.88: https://10.36.51.133/api/v2/agent-diagnostics/2022-08-02-16-18-5
Aug 2, 2022, 7:20:14 PM	ERROR	Did not receive all UPLOAD FILES responses after 1m8s. 1 agents did not respond.
Aug 2, 2022, 12:23:40 PM	ERROR	Could not upload files for agent 10.36.51.88: write /tmp/keysight/portmanager/diagcache//2022-08-02-09-23-38
Aug 2, 2022, 12:09:18 PM	ERROR	Could not upload files for agent 10.36.51.88: write /tmp/keysight/portmanager/diagcache//2022-08-02-09-09-15
Aug 2, 2022, 10:52:26 AM	INFO	CSV reports successfully generated for wireless-de51d273-abfb-40f2-a9fb-ba353ce1f6e7.
Aug 2, 2022, 10:52:24 AM	INFO	Generating CSV reports for wireless-de51d273-abfb-40f2-a9fb-ba353ce1f6e7.
Aug 2, 2022, 10:16:50 AM	ERROR	The following agents are offline and cannot be rebooted: 10.36.51.98.
Aug 2, 2022, 10:13:53 AM	ERROR	The following agents are offline and cannot be rebooted: 10.36.51.98.
Aug 2, 2022, 7:54:51 AM	INFO	CSV reports successfully generated for wireless-aa1623cc-bf11-4a16-9cf8-2ffff63aae01.
Aug 2, 2022, 7:54:50 AM	INFO	Generating CSV reports for wireless-aa1623cc-bf11-4a16-9cf8-2ffff63aae01.
Aug 1, 2022, 5:40:59 PM	INFO	Licenses successfully activated

Collect Diagnostics

DuSIM diagnostics tool is used to collect debug logs and other essential information needed in troubleshooting any encountered issues.

To collect diagnostics, do the following:

1. Click on **Collect Diagnostics** in the **Settings** menu. Select the Help icon in the title bar. The **Diagnostics** window appears.



2. If needed, select the optional components to include in the diagnostics report.
3. Select the log level used to collect diagnostics. Available options are:
 - **ERROR** - Designates messages indicating that an error has occurred that impacts application stability.
 - **WARN** - Designates messages indicating that an error has occurred that potentially impacts application stability.
 - **INFO** - Designates informational messages that highlight the progress of the application at coarse-grained level.
 - **DEBUG** - Designates fine-grained informational events that are most useful for debugging the application.
4. Click **Generate**. The diagnostics procedure can take several minutes to complete. Once it is finished, a download link will be displayed.
5. Select the download link to retrieve the diagnostics report.

Index

A

Access Control 222

administrator

- change password 14
- initial login 14

Agent Management, accessing 222

agents

- clear ownership 64
- management 62
- Network Management window 65
- ownership 60
- reboot 64
- status of 62
- tags 63

C

customer assistance 3

I

inter-CU handovers 75

J

jumbo frames 53

L

License Manager, accessing 222

N

Network Management window 65

P

passwords

- admin, change 14

user, change 17

product support 3

S

software updates 222

statistics

- licensing stats 217
- view in real time 44

System Monitor 222

T

tags

- custom 63
- types 59

technical support 3, 222

U

updates 222

user

- accounts 219
- management 222
- preferences 222



© Keysight Technologies, 2022–2024

This information is subject to change
without notice.

www.keysight.com