

Keysight Open RAN Simulators, Cloud Edition 5.0

Cu Isolation

User Guide

Notices

Copyright Notice

© Keysight Technologies 2025

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 those 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 Cu Isolation overview	12
Cu Isolation feature summary	13
UI overview	13
Chapter 2 Initial administrator login	16
Chapter 3 User login and logout	19
Chapter 4 Build and run a test	20
Step 1: Create a new test config	21
Step 2: Configure Global Settings	23
Step 3: Configure DU-CP test nodes	23
Step 4: Configure DU-UP test nodes	24
Step 5: Configure CU-CP test nodes	26
Step 6: Configure CU-UP test nodes	27
Step 7: Configure Core settings	27
Step 8: Configure DN settings	28
Step 9: Configure IMS settings	28
Step 10: Configure eNodeB node	28
Step 11: Configure mobile device definitions	29
Step 12: Create Scenario Groups	30
Step 12.1: Add and manage Scenario Groups	31
Step 12.2: Configure mobility	32
Step 12.3: Create Test Suites	34
Step 12.4: Defining parallel procedures	36
Step 13: Configure UEs	38
Step 14: Start the test	40
Step 15: View real-time test results	41

Chapter 5 Global Settings	43
Access Global Settings	45
Technical Spec Version	46
Node Start/Stop Rates settings	46
DNS Settings	46
Advanced Settings	48
DNNs panel	55
DNN configuration settings	55
Session AMBR configuration settings	58
ePCO configuration settings	58
Traffic Control Settings configuration	60
Impairment Settings	62
QoS Flows panel	63
QoS Flows configuration settings	63
QoS Flow Packet Filter configuration settings	67
QoS Flow Max Packet Loss Rate settings	68
QoS Flow ARP configuration settings	68
QoS Flow MBR configuration settings	69
QoS Flow GBR configuration settings	69
DRBs	69
TM Settings	70
Override Milenage Constants	71
Customer Parameters	72
CA Certificates Settings	72
Global Playlists	72
Chapter 6 Assign and manage agents	74
About traffic agents	75
Assigning agents to nodes	76
Agent management	78
Network Management	81
Distribution Mode feature	82

Chapter 7 DU-CP configuration settings	85
DU-CP Range panel	86
DU-CP RANGE panel	87
Cells settings	89
Measurement Timing Configuration	91
F1-CP Interface Settings	92
DU-PROCEDURE RANGE panel	99
Chapter 8 DU-UP configuration settings	101
DU-UP RANGES panel	102
DU-UP Range panel	103
Chapter 9 gNB CU-CP configuration settings	110
CU-CP Ranges panel	111
CU-CP Range settings	112
Settings panel	114
Cells settings	116
F1-CP Interface Settings	119
X2-C Interface Settings	119
Xn-C Interface Settings	120
CU-CP KIN Interface settings	121
Chapter 10 gNB CU-UP configuration settings	122
CU-UP RANGES panel	123
CU-UP Range settings	124
F1-UP settings	126
CU-UP KIN Interface Settings	128
Passthrough interface configuration	129
Chapter 11 eNodeB configuration settings	131
eNodeB RANGES panel	132
eNodeB RANGE panel	133
Cells settings	134
X2-C Interface Settings	135
X2-U Interface Settings	141

S1-C Interface Settings	142
S1-U Interface Settings	148
Chapter 12 Core configuration settings	151
Core Settings	152
N6/SGi interface settings	153
Core Ranges settings	154
AMF Ranges configuration settings	155
AMF node settings	156
AMF N2 interface settings	160
UPF Ranges configuration settings	160
UPF N3/S1-u/S5-u interface settings	161
MME Ranges configuration settings	162
MME node settings	163
MME S1 interface settings	165
SGW Ranges configuration settings	166
SGW S1-u interface settings	168
SEG Ranges configuration settings	168
SEG interface settings	172
N3IWF Ranges configuration settings	173
N3IWF interface settings	180
Chapter 13 IMS configuration settings	184
CSCF Range panel	184
Media Function Range panel	186
Chapter 14 DN configuration settings	187
DN Ranges panel	187
DN Range panel	188
DN N6 interface settings	189
DN routes settings	190
DN User Plane	190
DN Attacks	192
DN Stateless UDP Traffic	192

Data Traffic	193
DN Voice Traffic	197
DN Video OTT Traffic	209
DN DNS Server Traffic	214
DN Predefined Applications Traffic	216
DN Capture Replay	216
DN Synthetic	218
DN UDG	220
DN Throttling settings	222
Chapter 15 UE configuration settings	223
UE panel	224
UE RANGE settings	226
Identification settings	228
UE Security settings	228
UE ESM settings	230
UE EMM settings	232
UE NR Provisioning	234
UE Core Settings	235
Subscribed AMBR settings	247
UE DNNs Config	247
SMS Configuration	250
Untrusted WiFi Settings	251
Network Slicing settings	254
UE NSSAI settings	254
UDM SNSSAI Mappings	255
UE Device settings	257
Chapter 16 UE Test Objective settings	259
Control Plane Objective	260
About primary objectives	260
Secondary Control Plane Objective	262
Handover	263

Paging	265
Enter/Exit Idle	266
Create/Delete QoS Flows	266
Create/Delete PDU Sessions	269
SMS	270
User Plane Objectives	271
Stateless UDP Traffic	272
Data Traffic	274
Voice Traffic	280
Video OTT Traffic	296
DNS Client Traffic	301
ICMP Client	304
Capture Replay	304
Synthetic	307
UDG	309
Attacks	314
REST API Client	319
Predefined Applications Traffic	322
Applications	324
Application Advanced Settings	327
TCP Settings	329
TLS Settings	330
RTP Settings	333
Chapter 17 Scenario and Scenarion Groups settings	334
Mobility settings	336
Test Suite settings	339
Test procedures for SA	340
Deregistration	341
PDU Session Establish	342
PDU Session Release	344
Registration	346

Service Request	347
Test procedures for NSA tests	348
Attach	349
Detach	350
ENDC Configuration Update	351
EPS Bearer Activation	352
EPS Bearer Deactivation	353
Inter eNB Handover	354
PDN Connection Activation	355
PDN Connection Deactivation	357
SCG Release	359
SGBN Addition	360
MeNB Initiated SGBN Change Request	361
Test procedures for SA and NSA	362
Application Traffic	363
Delay	364
DU Initiated Release	365
NR-U Modification Request	366
UE Context Modification	367
IRAT Handover (LTE to NR)	368
Chapter 18 Manage and use test sessions	370
Save test sessions	371
Manage test sessions	372
Import and export sessions	376
Delete configs and sessions	378
Chapter 19 Manage Cu Isolation licenses	380
Licensing Requirements	381
License Manager	382
License server	384
Chapter 20 Manage Cu Isolation users	385
Chapter 21 Cu Isolation title bar settings	388

Chapter 22 Troubleshooting	391
View Notifications and Test Events	392
Collect Diagnostics	394
Appendix A Predefined Applications	A
Appendix B Cu IsolationApplication Actions	O
Index	BS

CHAPTER 1

Cu Isolation 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 Cu Isolation is a cloud-native solution designed to fully surround the gNB Central Unit (CU) with gNB Distributed Units (DUs) and a core network or DN. It simulates user plane and control plane traffic flowing over the F1 interface from a simulated gNB-DU to your gNB-CU (the DUT), and it responds to traffic sent from your DUT to the simulated gNB-DU.

It also simulates user plane and control plane traffic flowing over the N3 interface from a simulated Core to your gNB-CU (the DUT), and it responds to traffic sent from your DUT to the simulated Core.

Since this is complete wrap around solution, Cu Isolation also simulates UE/Cells/RU within it, and provides full NAS/RRC and PDCP functionalities.

Chapter contents:

Cu Isolation feature summary	13
UI overview	13

Cu Isolation feature summary

Cu Isolation 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).

Cu Isolation feature summary:

- Supports testing in 5G SA and NSA mode, and supports simulated eNB while in NSA mode.
- Features a web-based user interface (UI) through which you manage all aspects of your Cu Isolation 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 supported platform, which includes all major private and public cloud platforms, as well as over container services.

The supported platforms include:

- private clouds: VMware ESXi 6.5 and ESXi 6.7
- Supports multi-thread control plane process flows.
- Provides extensive control plane and user plan statistics coverage.
- Provides support for script-based impairments (Python scripts).

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 Cu Isolation UI are:

- [Dashboard page below](#)
- [Title bar and tool bars on the facing page](#)
- [Test Overview page on the facing page](#)
- [Configuration properties pages on page 15](#)
- [Statistics page on page 15](#)

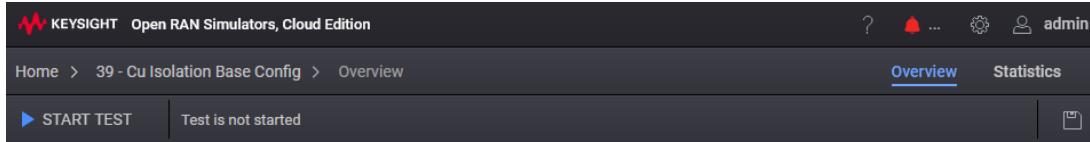
Dashboard page

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.

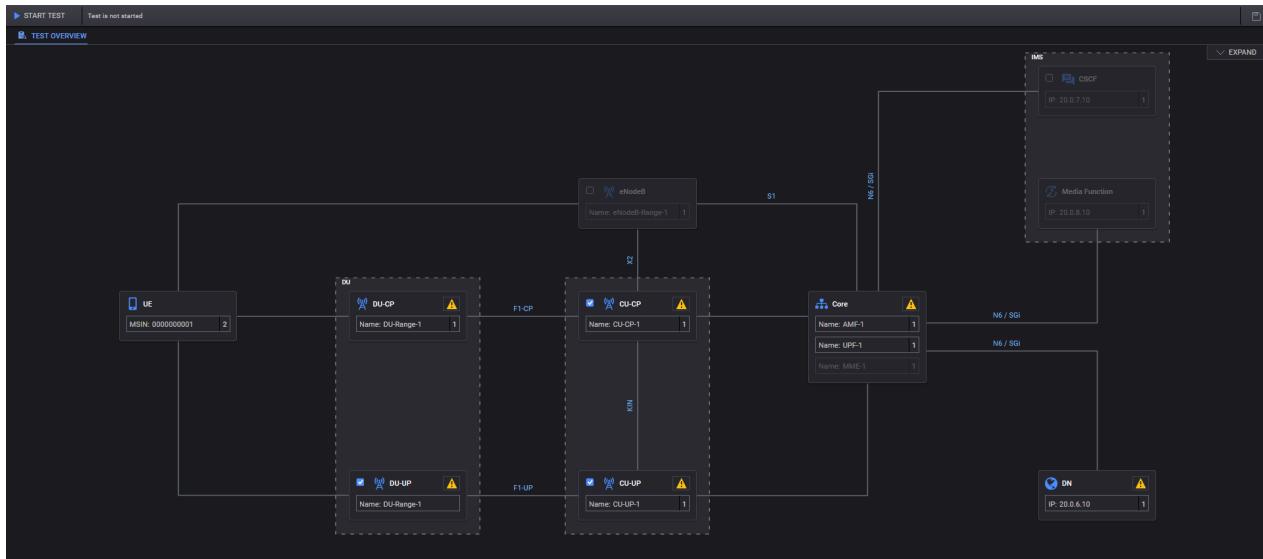


In addition to the information in this topic, refer to these topics for more information about the available tools and functions:

- [Cu Isolation title bar settings on page 388](#)
- [Save test sessions on page 371](#)

Test Overview page

When you open or create a test session based on any predefined, newly-created, or imported test configuration, Cu Isolation 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 test topology is an interactive graphical representation of the test network. From the topology, you access all of the configurable elements for the current test. These include the CU (which is represented as a CU-CP node and a CU-UP node), the DU (which is represented as a DU-CP node and a DU-UP node), the 5G core, the eNodeB, the IMS, the DN, and the user endpoints (UEs).

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 SCTP Connections, F1 setup, RRC procedure rates, NAS procedure rates, PDU sessions, 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 Cu Isolation 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 18](#)

Required information

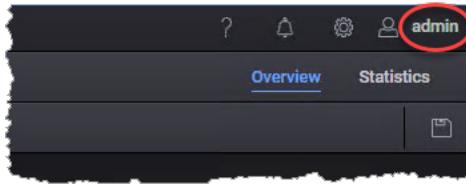
- The IP address that you set for the Cu Isolation web interface during deployment.
- The IP address of the license server.
The license server is shipped as a separate .ova file. After deploying the .ova file, you can access it using a web browser.
- Your Cu Isolation license activation codes (or entitlement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

Initial login and password change

Cu Isolation 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 Cu Isolation instance in your browser's address field.
Cu Isolation 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, Cu Isolation 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 5.0 title bar.



Keysight Open RAN Simulators, Cloud Edition 5.0 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 Cu Isolation deployment.

To activate your licenses:

1. Select **Licensing** from the setup menu (⚙).
2. Select **License Manager** from the **Licensing** menu. Cu Isolation opens the **License Manager** page.
3. To activate your licenses:
 - a. Select **Activate licenses**.
Cu Isolation 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 (⚙).
Cu Isolation 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 Cu Isolation users on page 385](#) for detailed information about user account management.

CHAPTER 3

User login and logout

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

Log in as a regular user

The user accounts that the Cu Isolation 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 Cu Isolation 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 5.0 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, Cu Isolation opens the dashboard.

Log out



To log out of Cu Isolation, go to **User Account** (on the title menu and select **Log Out** .

CHAPTER 4

Build and run a test

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

Chapter contents:

Step 1: Create a new test config	21
Step 2: Configure Global Settings	23
Step 3: Configure DU-CP test nodes	23
Step 4: Configure DU-UP test nodes	24
Step 5: Configure CU-CP test nodes	26
Step 6: Configure CU-UP test nodes	27
Step 7: Configure Core settings	27
Step 8: Configure DN settings	28
Step 9: Configure IMS settings	28
Step 10: Configure eNodeB node	28
Step 11: Configure mobile device definitions	29
Step 12: Create Scenario Groups	30
Step 12.1: Add and manage Scenario Groups	31
Step 12.2: Configure mobility	32
Step 12.3: Create Test Suites	34
Step 12.4: Defining parallel procedures	36
Step 13: Configure UEs	38
Step 14: Start the test	40
Step 15: View real-time test results	41

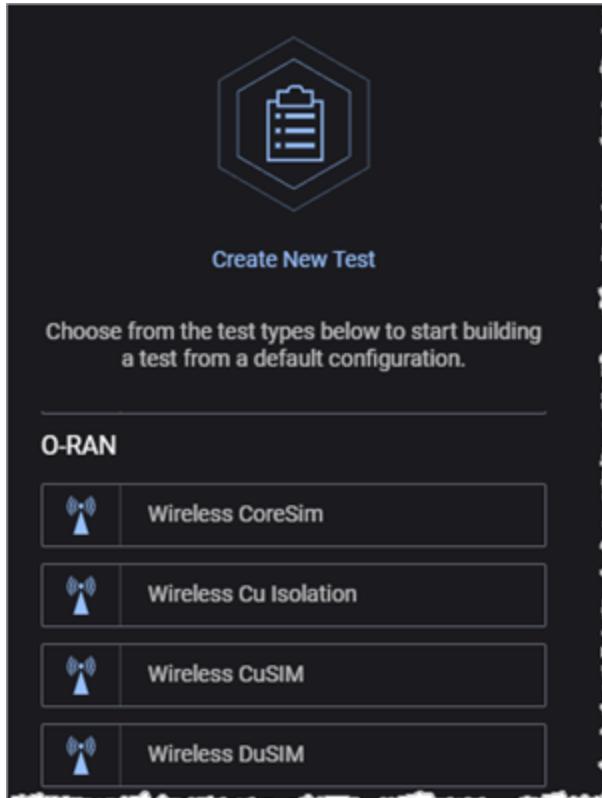
Step 1: Create a new test config

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 Cu Isolation.
2. In the Dashboard page, select the **Wireless Cu Isolation** template from the **Create New Test** panel. For example:

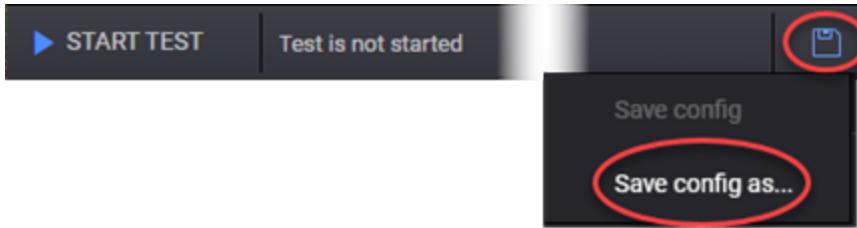


Cu Isolation opens the **Test Overview** page, which includes the graphical representation of the test topology. By default, SA topology is activated. You need to select NSA or CU-Simulated node for another network topology.

Cu Isolation 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:

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



Cu Isolation opens the **Save config as** dialog.

- 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 370](#) 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 Cu Isolation 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 5.0 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** (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.

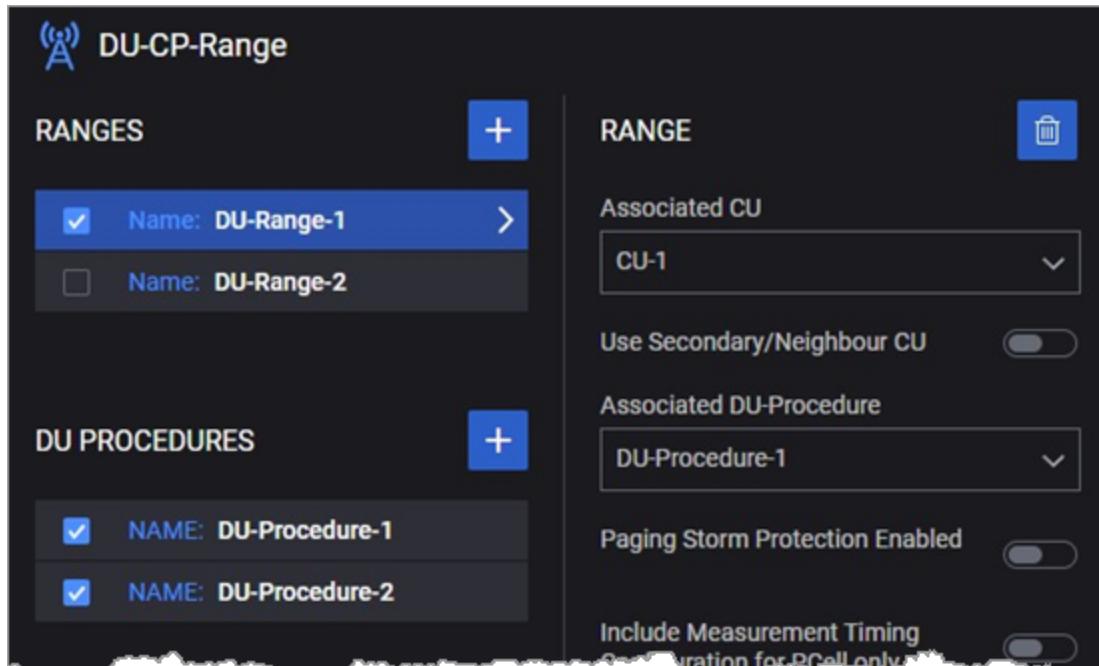
Refer to [Global Settings on page 43](#) for a description of all of the settings.

Step 3: Configure DU-CP test nodes

The Cu Isolation 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.
Cu Isolation 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:



3. Configure each of the settings, which are described in [DU-CP configuration settings](#).

4. To add and configure additional DU-CP ranges:

- Return to the DU-CP **RANGES** panel.
- Click the **Add Range** button.

NOTE

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

- Configure the settings for the new range.

5. To select or deselect a range for the test:

- Return to the DU-CP **RANGES** panel.
- Click the **Select** check box to toggle the range between *Selected* and *Deselected*, as required.

6. To delete a DU-CP range:

- In the DU-CP **RANGES** panel, click the range to open its properties panel.
- Click the **Delete Range** button. Cu Isolation deletes the range from your test config.

NOTE

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

Step 4: Configure DU-UP test nodes

The Cu Isolation 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

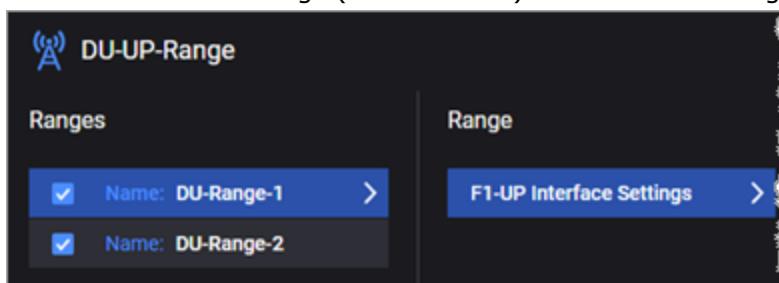
Cu Isolation manages DU-UP ranges as follows:

- Cu Isolation automatically creates one DU-UP range for each DU-CP range that you configure in the test.
- If you delete a DU-CP range, Cu Isolation 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, Cu Isolation does not deselect the corresponding DU-CP range.

How to configure DU-UP nodes

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

- Select **DU-UP** from the topology window.
- Cu Isolation opens the DU-UP **RANGES** panel.
- 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 103](#).
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 5: Configure CU-CP test nodes

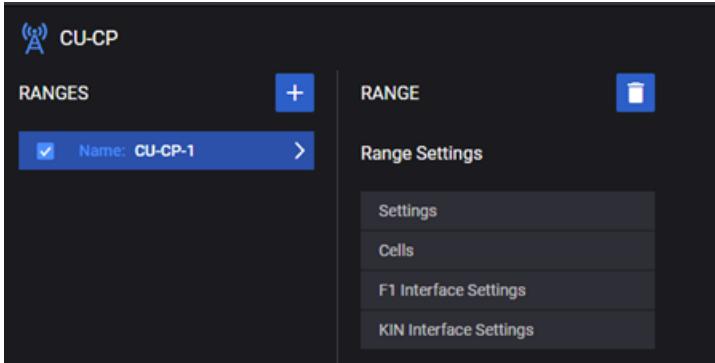
The Cu Isolation test topology includes a representation of the simulated CU nodes in your test configuration. Each CU node is structured as two units: CU-CP and CU-UP.

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

1. Select **CU-CP** from the topology window.

Cu Isolation opens the CU-CP **RANGES** panel. A new test will have one CU-CP range; you can add additional ranges.

2. Select the name of a range (such as CU-CP-1) to access the configuration settings. For example:



3. Configure each of the settings, which are described in [gNB CU-CP configuration settings](#).

Step 6: Configure CU-UP test nodes

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

About CU-UP ranges

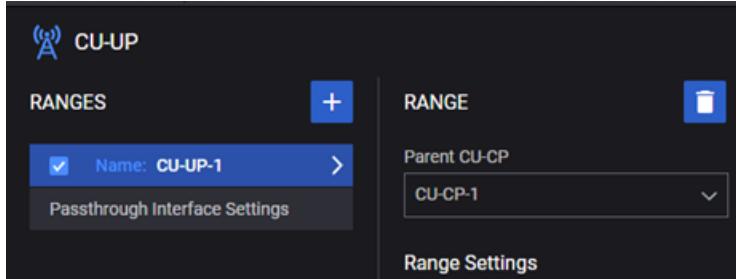
Cu Isolation manages CU-UP ranges as follows:

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

How to configure CU-UP nodes

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

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



3. Configure each of the settings, which are described in [CU-UP Range settings on page 124](#).
4. To select or deselect a range for the rest:
 - a. Return to the CU-UP **RANGES** panel.
 - b. Select the **Select** check box to toggle the range between *Selected* and *Deselected*, as required.
5. To configure a passthrough interface in a test, refer to [Passthrough interface configuration on page 129](#).

Step 7: Configure Core settings

In the 5G standalone (SA) topology, CoreSim simulates control plane traffic from the AMF over the N1 and N2 interfaces, and user plane traffic from the UPF over the N3 interface towards the NG-RAN.

Configure each of the settings, as described in [Core configuration settings](#).

Step 8: Configure DN settings

Data Networks (DN) represents one of the entities in the 5G core network architecture. DN interfaces enable access to the public Internet, operator services, and other external data networks.

Configure each of the settings, as described in [DN Range panel](#).

Step 9: Configure IMS settings

The IP Multimedia Subsystem (IMS) is a standards-based architectural framework for delivering multimedia communications services such as voice, video and text messaging over IP networks. IMS enables secure and reliable multimedia communications between diverse devices across diverse networks.

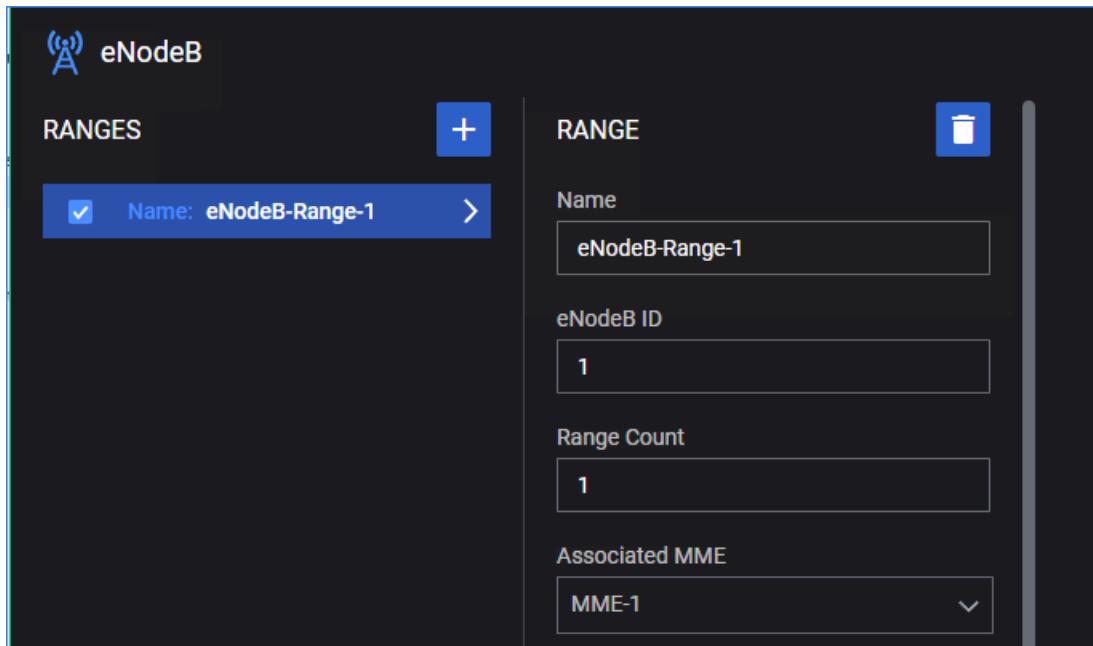
IMS has two important components:

- [Call Session Control Function \(CSCF\)](#) – the core of the IMS architecture, responsible for controlling sessions between endpoints (referred to as terminals in the IMS specifications) and applications.
- [Media Function](#)

Configure each of the settings, as described in [IMS configuration settings](#).

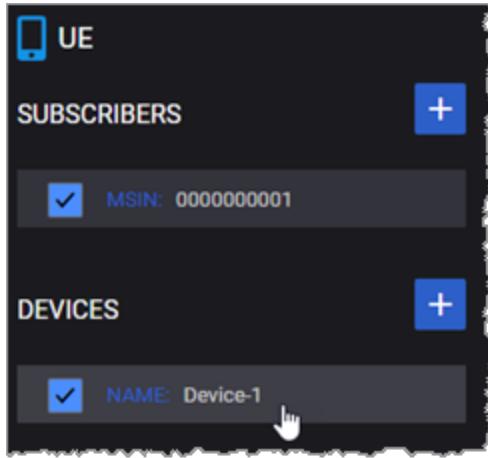
Step 10: Configure eNodeB node

If you are configuring an NSA mode topology, you must select eNodeB node. eNodeB does not need any Agent specifically to assign. It runs on previously assigned agents for DU-CP node.



Step 11: Configure mobile device definitions

In a Cu Isolation 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:

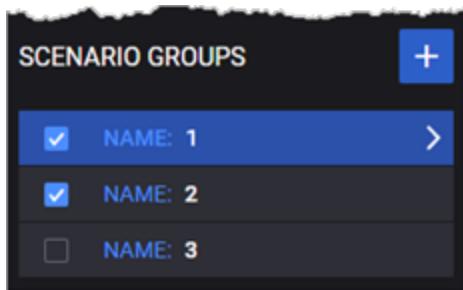
1. Select **UE** from the Cu Isolation topology window.
Cu Isolation opens the top-level (leftmost) UE properties window.
2. From the UE panel, click a **DEVICES** range (such as Device-1) to open its properties panel.
3. Configure the device settings, as described in [UE Device settings](#).
4. To add 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. Cu Isolation deletes the range from your test config.

Step 12: 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 and Scenarion Groups settings on page 334](#) for detailed descriptions of the configuration settings.

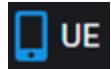


SCENARIO GROUPS define the detailed control plane traffic that enables the subscribers to access the network and successfully transmit user plane traffic.

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

Step 12.1: Add and manage Scenario Groups	31
Step 12.2: Configure mobility	32
Step 12.3: Create Test Suites	34
Step 12.4: Defining parallel procedures	36

Step 12.1: 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 (Cu Isolation assigns each group a number). Cu Isolation 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. Cu Isolation 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. Cu Isolation immediately removes it from the test configuration.

Step 12.2: Configure mobility

Each Scenario Group can configure UE mobility actions.

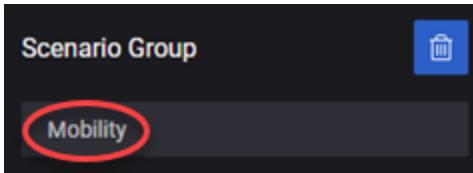
1. Click **UE** in the topology window to open the UE properties panel.



2. Select the **Scenario group** for which you are configuring mobility.

Cu Isolation opens its properties panel, which is where you access the Mobility settings.

3. Select **Mobility** from the Scenario group properties panel.



Cu Isolation opens a new panel to display the **Mobility** settings (which are described in [Mobility settings on page 336](#)).

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**.

Cu Isolation 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**.

Cu Isolation 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. Cu Isolation adds an **NR** link to the panel.

- b. Click the **NR** link. Cu Isolation 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, Cu Isolation 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, Cu Isolation chooses the DUs with which the UEs will perform the initial attach and handovers. With Cu Isolation automatically making these choices, it is not difficult to scale the mobility simulation for thousands of UEs and thousands of DUs.

Step 12.3: Create Test Suites

Cu Isolation 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 36](#)

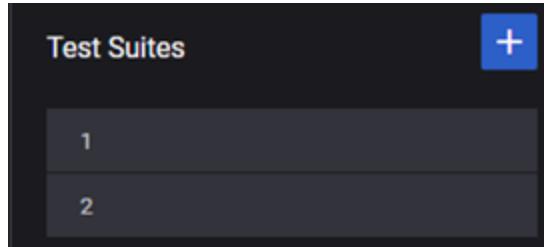
Accessing the Test Suite settings

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 (Cu Isolation assigns each group a number). Cu Isolation 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. Cu Isolation 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 339](#) for a description of the Test Suite configuration settings.

Delete a Test Suite

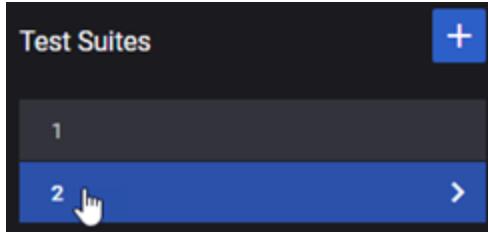
To delete a Test Suite from a selected Scenario Group:

1. Select the Scenario Group from which you will delete the Test Suite.
2. Click the **Test Suite** number to select it. Cu Isolation 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 Cu Isolation 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.

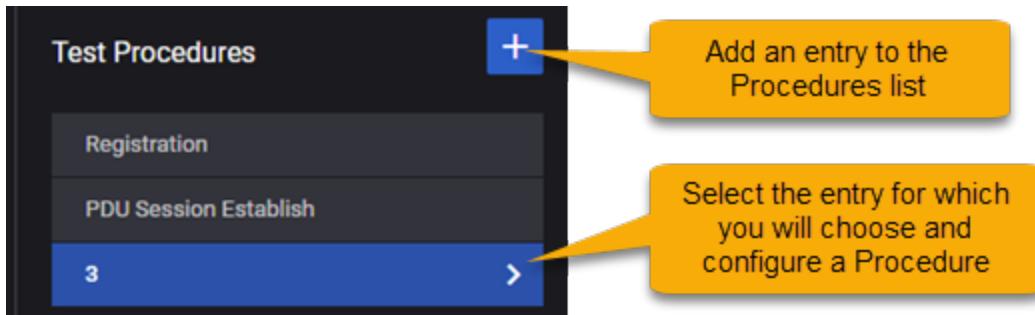


Cu Isolation opens the **Test Suite** properties panel.

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 339](#) for detailed descriptions of these properties.

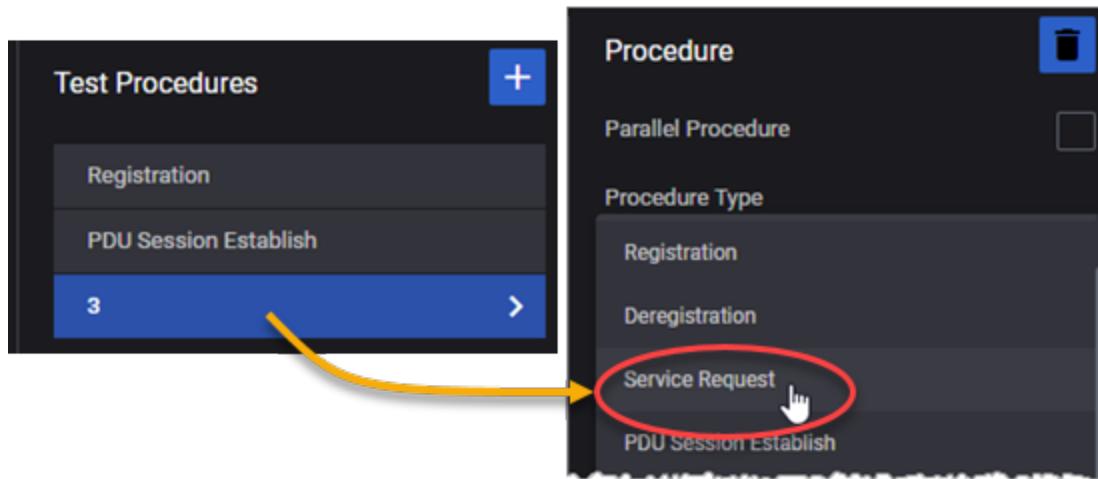
3. Select and configure the specific procedures that this test suite will execute:



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

Cu Isolation opens the **Procedure** panel.

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



Cu Isolation 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 340](#), [Test procedures for NSA tests on page 348](#), and [Test procedures for SA and NSA on page 362](#) 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](#).

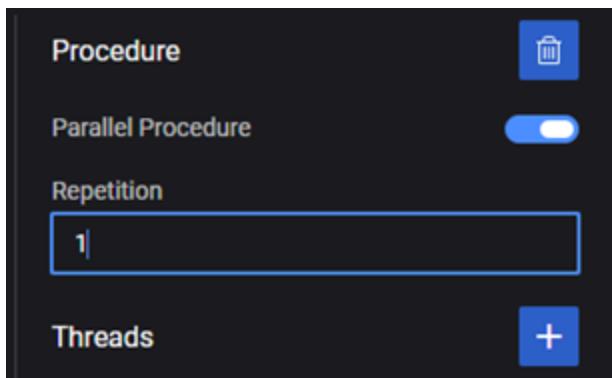
Step 12.4: Defining parallel procedures

Each Cu Isolation 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.

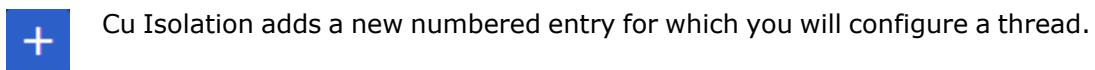
Enable the *Parallel Procedure* option and set the *Repetition* value.



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

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

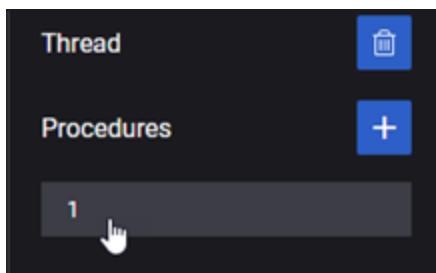
Click the **Add Thread** button.



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

Cu Isolation 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.



Cu Isolation 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).

Cu Isolation 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 340](#), [Test procedures for NSA tests on page 348](#), and [Test procedures for SA and NSA on page 362](#) for a description of the Procedure configuration settings.

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

Step 13: Configure UEs

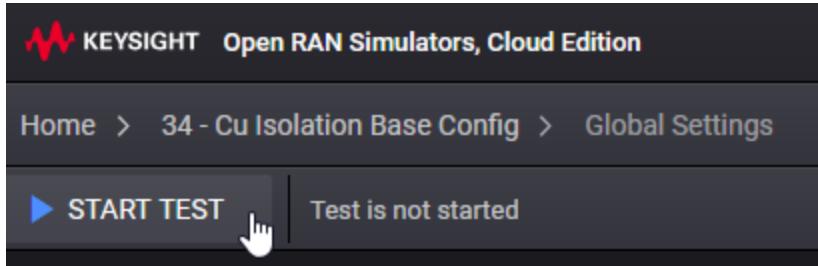
To configure one or more ranges of mobile UE definitions for a test:

1. Select **UE** from the Cu Isolation topology window.
Cu Isolation 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.)
Cu Isolation 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, Security settings, ESM settings, EMM settings, DNN settings, Network Slicing settings, NR provisioning and more.
Refer to [UE configuration settings on page 223](#) for detailed descriptions.
 - d. Configure the Protocol Configuration Options in the ESM settings:
 - i. From the **ESM Parameters** settings, 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 **Control Plane** (in the **Objectives** section).
Cu Isolation opens the **Control Plane** panel.
 - ii. Select the **Objective Type** that you need for this range. Then assign and configure **Secondary Objectives**, if required.
Refer to [UE Test Objective settings on page 259](#) for a description of the properties that you can configure for each of the secondary objective types.
 - iii. In the **RANGE** panel, click **User Plane** (in the **Objectives** section).
Cu Isolation opens the **User Plane** panel.
 - iv. 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 259](#) 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.
Cu Isolation opens that UE **RANGE** panel.
 - b. Click the **Delete Range** button. Cu Isolation deletes the range from your test config.

Step 14: 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 Cu Isolation tool bar displays the test status throughout its execution progress. In addition, each test session tile (located on the Cu Isolation 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.

Cu Isolation 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, Cu Isolation 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. Cu Isolation 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 15: View real-time test results

When you successfully start a test, Cu Isolation 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:

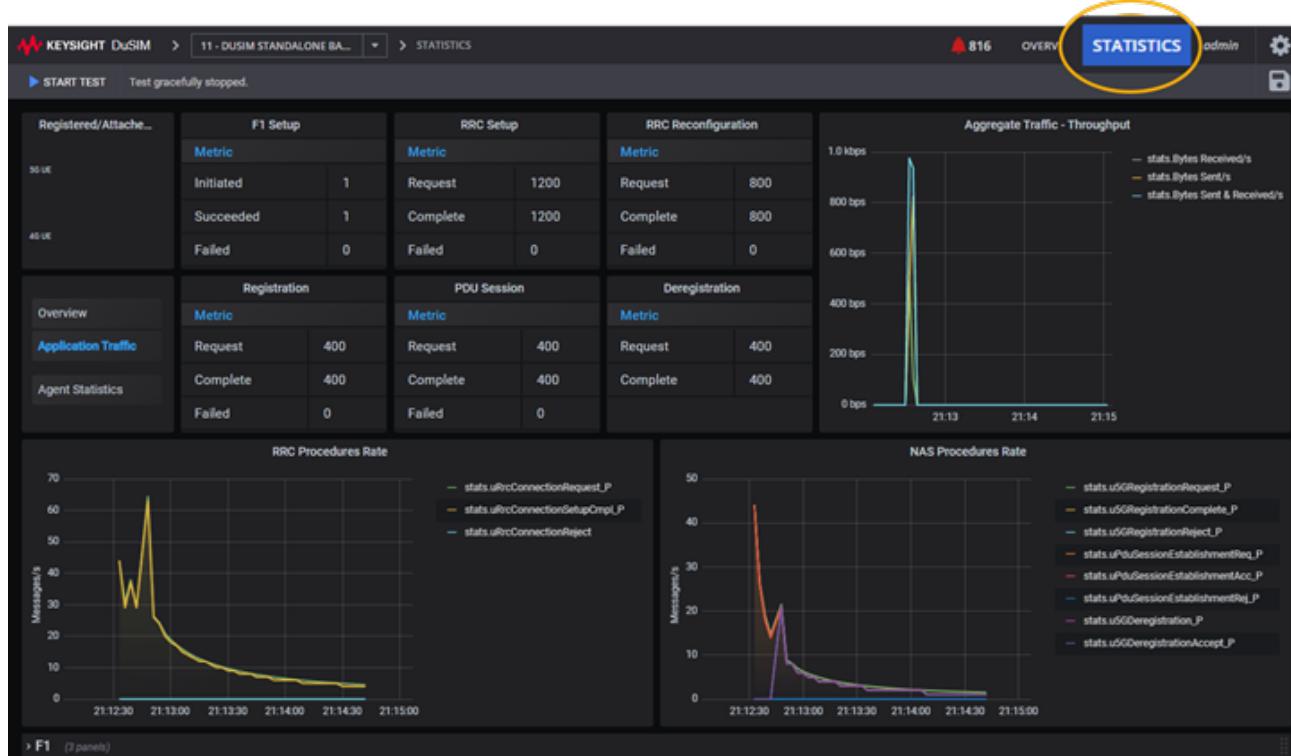
- F1 Setup: number of procedures initiated, succeeded, and failed.
- RRC Setup: number of procedures initiated, succeeded, and failed.
- RRC Reconfiguration: number of procedures initiated, succeeded, and failed.
- Registration: number of procedures initiated, succeeded, and failed.
- PDU Session: number of procedures initiated, succeeded, and failed.
- Dereistration: 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 Cu Isolation 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	45
Technical Spec Version	46
Node Start/Stop Rates settings	46
DNS Settings	46
Advanced Settings	48
DNNs panel	55
DNN configuration settings	55
Session AMBR configuration settings	58
ePCO configuration settings	58
Traffic Control Settings configuration	60
Impairment Settings	62
QoS Flows panel	63
QoS Flows configuration settings	63
QoS Flow Packet Filter configuration settings	67
QoS Flow Max Packet Loss Rate settings	68
QoS Flow ARP configuration settings	68
QoS Flow MBR configuration settings	69
QoS Flow GBR configuration settings	69
DRBs	69
TM Settings	70
Override Milenage Constants	71
Customer Parameters	72

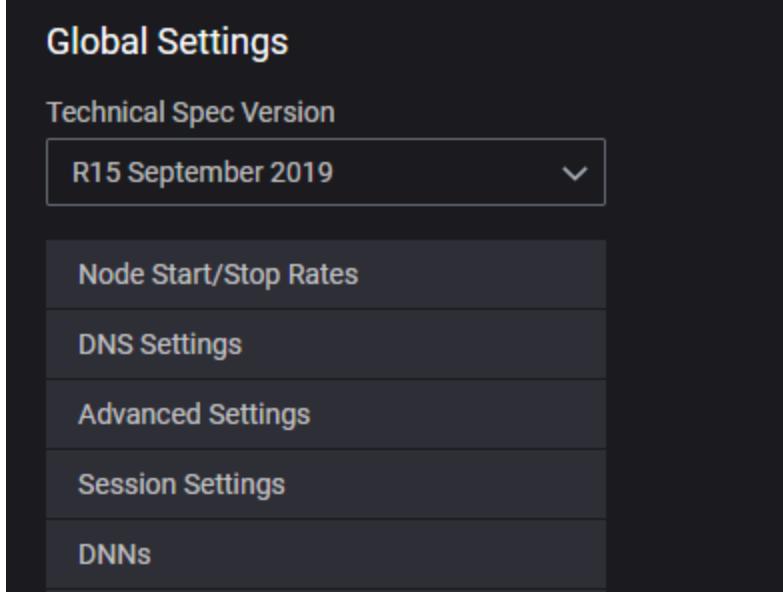
CA Certificates Settings	72
Global Playlists	72

Access Global Settings

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

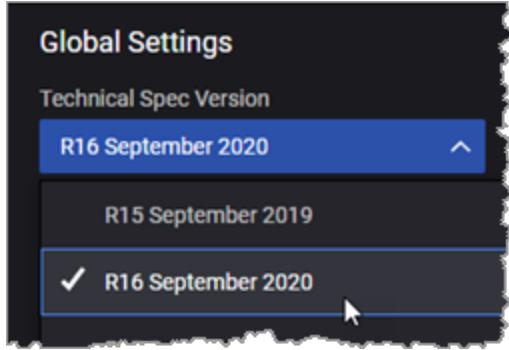
1. Select the **Test Overview** tab.
2. Click **Expand** if the **Test Overview** section is collapsed.
3. Click the **Edit** button on the Global Settings section.

This opens the **Global Settings** panel.



Technical Spec Version

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



Node Start/Stop Rates settings

The following table describes the settings that are available on the Node Start/Stop Rates. These include settings with which you control the Stream Control Transmission Protocol (SCTP) connection rates between NG-RAN and AMF. (SCTP—which operates in the transport layer of the NG-C signaling bearer—provides for the reliable transport of signaling messages.)

Setting	Description
<i>Node Start:</i>	
Rate	Set the desired start rate for SCTP connections between the NG-RAN and the AMF (connections per second). Measured in procedures per second if Distributed over (s) is not modified.
Distribution Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
<i>Node Stop:</i>	
Rate	Set the desired start rate for SCTP connections between the NG-RAN and the AMF (connections per second). Measured in procedures per second if Distributed over (s) is not modified.
Distribution Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.

DNS Settings

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

Setting	Description
Cache	The amount of time (in milliseconds) the local DNS stores the address information.

Setting	Description
Timeout (ms)	
<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](#)
- [KIN Interface Settings](#)
- [Response Cache Settings](#)

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 Control Plane Advanced Stats	Select this option to enable control plane latency statistics.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: <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)	This option becomes available only when <i>Automated Polling Interval</i> option is disabled. It allows you to set a custom polling interval.
Ignore offline Agents at Runtime	When enabled, if an agent losses connection to the Middleware during a test, the test will not stop, but continue without that agent.

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
	which helps in debugging on the selected component. Select one or more components from the drop-down list.

F1APSM - F1 Application Protocol (F1AP) State Machine

Setting	Description
Log level	Select one of the options: <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	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. Select one or more components from the drop-down list.

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	Select one of the options: <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	<p>Specify the number of secondary processes.</p> <p>The TM works in primary-secondary process module , where primary processes distributes work on secondary processes.</p> <p>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.</p>

TM Adaptor

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.

TM ENB

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.

Nimbus Adaptor

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

Setting	Description
	<p>impacts system stability.</p> <ul style="list-style-type: none"> • 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.

Traffic Settings

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

Setting	Description
<i>GTPU Source Port:</i>	
Start	The starting source port number. This value is incremented by 1 for each GTP-U source port that is configured.
Count	The number of GTP-U source ports required.
<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.
<i>Traffic Control:</i>	
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.
Enable Jumbo Frame	<p>Enable this option if your test traffic requires the use of jumbo frames (Ethernet frames with more than 1500 bytes of payload).</p> <p>When you enable this option, you can configure any of the MTU parameters in the test to any valid jumbo frame size (up to 9,000 bytes).</p>
Enable IxStack L4 Port Randomization	Select this option to enable IxStack L4 Port Randomization.
Enable UDP Port Recycling	Select this option to enable IxStack UDP Port Recycling.
Enable TCP Port Recycling	Select this option to enable IxStack TCP Port Recycling.

Setting	Description
Enable ICMP Responses	Select this option to enable it. This will permit requests and responses to ICMP packets on subscribers addresses (it will have a significant memory impact on server nodes - AMF, UPF).

KIN Interface Settings

The traffic agents of the Cu Isolation 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	
IP Prefix Length	

Response Cache Settings

During performance testing scenarios, it is possible that not all responses are received by the client. The client initiates messages retries when it is not receiving responses. When a message retry reaches the server, the response is sent again faster and no additional load is put on the server, because the response message is already stored. There is no need to construct the response message again.

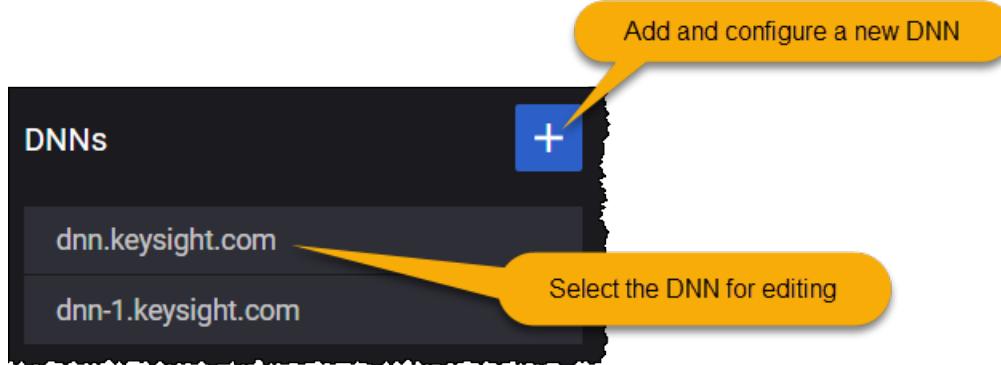
A rotation interval higher than the retry timer on the client node must be configured in order to still have the responses stored when a message retry arrives on the server node.

The following table describes the settings on the Response Cache pane.

Setting	Description
Enable response cache for GTPv2 and PFCP protocols	When this option is enabled, the server node will store the GTPv2 and PFCP Response messages for a period of time equal to Rotation Interval (in seconds).
Rotation interval	The period of time (in seconds) for which the server node will store the GTPv2 and PFCP Response messages. After this interval expires, the stored messages are discarded.

DNNs panel

To access the DNN configuration settings, select **DNNs** from the the **Global Settings** panel. Cu Isolation opens the **DNNs** panel from which you can add and edit DNN definitions:



The properties for a DNN are organized into the following groups of configuration settings:

DNN configuration settings	55
Session AMBR configuration settings	58
ePCO configuration settings	58
Traffic Control Settings configuration	60

DNN configuration settings

You create and manage Data Network Names (DNNs) for your test network in the **Global Settings** section of the **Test Overview**. 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>DNN:</i>	
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. • 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>

Setting	Description
	<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 [start_value-end_value,increment].</p> <p>NOTE The start_value and end_value must have the same length. For example, we can configure dnn[008-999,1] and obtain dnn008,dnn009,...,dnn998,dnn999. Syntaxes dnn[8-999,1] or [008-1000,1] are not valid as the start and end value lengths are different.</p> <p>The start value is mandatory. Omitting certain parameters results in behaviors as exemplified below:</p> <ul style="list-style-type: none"> • dnn[4-9,] an implicit increment of 1 is used • dnn[4-9] as above • dnn[4-,1] is used as dnn[4-9,1], 9 being the maximum value with the configured length, length of 1 in this case • dnn[4-,] as above • dnn[4-] as above • dnn[4] as above <p>UEs will use the DNN values from the pool in a round robin manner.</p> <p>IMPORTANT If multiple sequence generators are configured and their pools overlap (for example: dnn[000-600,1].keysight.com dnn[500-999,1].keysight.com), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the start_value (they might start with an intermediate value in the second pool).</p>
PDU Type	Select the desired PDU type: IPv4, IPv6 or IPv4v6.
QoS Flows IDs	<p>Select the QoS Flows ID(s) from the drop-down list. Each DNN should contain at least the default flow (the default flow is unique per each DNN). In addition, zero or more dedicated flows can be associated to each DNN.</p> <p>For more details about QoS Flow configuration, refer to QoS Flow configuration settings.</p>

Setting	Description
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> • SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. • SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) 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 in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
EPS Interworking	Enable this option if the UE subscription data indicates support for interworking with EPS for this DNN.
Is Emergency DNN	When this option is enabled, if an UE range has mapped this type of DNN, it will perform an emergency PDU Session.
MPS Priority	Enable this option if the DNN will support subscription to MPS priority service. The priority applies to all traffic on the PDU Session.
Dual Registration Mode	When enabled, it transfers this session to the other RAT in dual registration mode. If the session does not exist, it will be created in the other RAT.
MPS Priority Level	Specify the Multimedia Priority Services (MPS) priority level. This is the relative priority level for MPS.
IMS Signaling Priority	Specify the IP Multimedia Subsystem (IMS) signaling priority. This value indicates subscription to IMS signaling priority service. The priority applies only to IMS signaling traffic.
Session Rule Name	Set the session rule name.
GBR	<i>Select this option to open the GBR panel.</i>
Guaranteed Bit Rate Uplink	Specify the guaranteed bit rate for the uplink traffic.
Guaranteed Bit Rate Downlink	Specify the guaranteed bit rate for the downlink traffic.
Session AMBR	<i>Select this option to open a new panel that contains the Session AMBR settings. These settings are described in Session AMBR configuration settings.</i>
ePCO	<i>Select this option to open the extended protocol configuration options panel.</i>

Setting	Description
	<i>These settings are described in ePCO configuration settings.</i>
Traffic Control Settings	Select this option to open the traffic control settings panel. These settings are described in Traffic Control Settings configuration .

Session AMBR configuration settings

About Session AMBR ...

5G QoS enforcement and rate limitation policies utilizes Aggregate Maximum Bit Rate (AMBR) values to limit the amount of traffic flowing through the 5GS for a given UE. Every PDU session specifies a per-session AMBR value that limits the aggregate bit rate that can be expected across all non-GBR QoS flows. The Session-AMBR is measured over an AMBR averaging window, which is a standardized value. Downlink Session-AMBR is enforced by the UPF, and uplink Session-AMBR is enforced by the UPF and the UE.

The following tables describes the Session AMBR configuration settings.

Parameter	Description
Session AMBR Uplink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Session AMBR Uplink unit	The unit in which the rate is expressed. The options range from Kbps to Tbps.
Session AMBR Downlink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) downlink rate.
Session AMBR Downlink unit	The unit in which the rate is expressed. The options range from Kbps to Tbps.

ePCO configuration settings

Configuration options for ePCO IE (extended Protocol Configuration Options IE) from PDU Session Establishment Request message and PDU Session Establishment Accept message.

Parameter	Description
Request DNS Server IP Address	Add DNS Server IPv4 Address Request or DNS Server IPv6 Address Request in the Extended Protocol Configuration Options IE included in PDU Session Establishment Request message. If required, enable this option.
Request P-CSCF IP address	Add P-CSCF IPv4 Address Request or P-CSCF IPv6 Address Request in the Extended Protocol Configuration Options IE included in PDU Session Establishment Request message. If required, enable this option.

Parameter	Description
Request IPv4 Link MTU	<p>Add IPv4 Link MTU Request in the Extended Protocol Configuration Options IE included in PDU Session Establishment Request message.</p> <p>If required, enable this option.</p>
DNS Server IPv4 Address	<p>If ePCO IE was received in PDU Session Establishment Request on CoreSim and DNS Server IPv4 Address Request was set, send this DNS IPv4 address in the ePCO IE in PDU Session Establishment Accept message if this field is not empty.</p> <p>NOTE If this field is empty and a DNS Name Server is configured in Global Settings > DNS Settings > DNS Name Servers, then this field will be populated with the first IPv4 address of the DNS Name Server(s) defined in Global Settings.</p> <p>NOTE If the DNS Name Server IPv4 address is updated in Global Settings > DNS Settings > DNS Name Servers while there is already a value set for DNS Server IPv4 Address, no update will be done on DNS Server IPv4 Address. If the new IPv4 DNS address is needed, the update in ePCO settings needs to be done manually.</p>
DNS Server IPv6 Address	<p>If ePCO IE was received in PDU Session Establishment Request on CoreSim and DNS Server IPv6 Address Request was set, send this DNS IPv6 address in the ePCO IE in PDU Session Establishment Accept message if this field is not empty.</p> <p>NOTE If this field is empty and a DNS Name Server is configured in Global Settings > DNS Settings > DNS Name Servers, then this field will be populated with the first IPv6 address of the DNS Name Server(s) defined in Global Settings.</p> <p>NOTE If the DNS Name Server IPv6 address is updated in Global Settings > DNS Settings > DNS Name Servers while there is already a value set in ePCO for DNS Server IPv6 Address, no update will be done on ePCO DNS Server IPv6 Address. If the new IPv6 DNS address is needed, the update in ePCO settings needs to be done manually.</p>
P-CSCF IPv4 address	<p>If ePCO IE was received in PDU Session Establishment Request on CoreSim and P-CSCF IPv4 Address Request was set, send this P-CSCF IPv4 address in the ePCO IE in PDU Session Establishment Accept message if this field is not empty.</p> <p>NOTE If this field is empty and the CSCF node is enabled and has an IPv4 address, then this field is automatically updated to the CSCF IPv4 address.</p> <p>NOTE If the IPv4 address of the IMS CSCF node is manually changed while there is already a value set for ePCO P-CSCF IPv4 address, this will not be automatically updated on ePCO P-CSCF IPv4 address. If the new CSCF address is needed, the update in ePCO settings needs to be done manually.</p>
P-CSCF IPv6 address	<p>If ePCO IE was received in PDU Session Establishment Request on CoreSim and P-CSCF IPv6 Address Request was set, send this P-CSCF IPv6 address in the ePCO</p>

Parameter	Description
	<p>IE in PDU Session Establishment Accept message if this field is not empty.</p> <p>NOTE If this field is empty and the CSCF node is enabled and has an IPv6 address, then this field is automatically updated to the CSCF IPv6 address.</p> <p>NOTE If the IPv6 address of the IMS CSCF node is manually changed while there is already a value set for ePCO P-CSCF IPv6 address, this will not be automatically updated on ePCO P-CSCF IPv6 address. If the new CSCF address is needed, the update in ePCO settings needs to be done manually.</p>
Link MTU value	If ePCO IE was received in PDU Session Establishment Request on CoreSim and IPv4 Link MTU Request was set, send this IPv4 Link MTU value in the ePCO IE in PDU Session Establishment Accept message.

Known limitations:

- ePCO is only supported on NG-RAN and CoreSim 5G.
- The options are only used for signaling, in order to avoid errors. There is no support for sending/receiving traffic according to this option.

Traffic Control Settings configuration

The Traffic Control Settings option offers the ability to use Traffic Control on a per DNN basis.

When enabled, after the Delay Between PDU Session Establishment and Suspend Traffic timer expires, Traffic Control specific messages will be sent from the UE IP address assigned for that specific PDU Session to the configured Remote IPv4 or Remote IPv6 peer address in order to stop downlink traffic. Downlink traffic will be resumed after the configured Suspend Traffic Interval expires.

The following tables describes the Traffic Control Settings parameters.

Parameter	Description
Traffic Control Settings	<i>By default, this option is disabled.</i> <i>Select the check box to enable it.</i>
Suspend Traffic Interval(s)	Set the value (in seconds) for this parameter.
Delay Between PDU Session Establishment and Suspend Traffic	Set the value (in seconds) for this parameter.
Remote IPv4	<p>Select:</p> <ul style="list-style-type: none"> •  - Select to add the remote IPv4 address. •  - Select to remove the remote IPv4 address.

Parameter	Description
Remote IPv6	<p>Select:</p> <ul style="list-style-type: none">•  - Select to add the remote IPv6 address.•  - Select to remove the remote IPv6 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 Cu Isolation 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 Cu Isolation.
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.

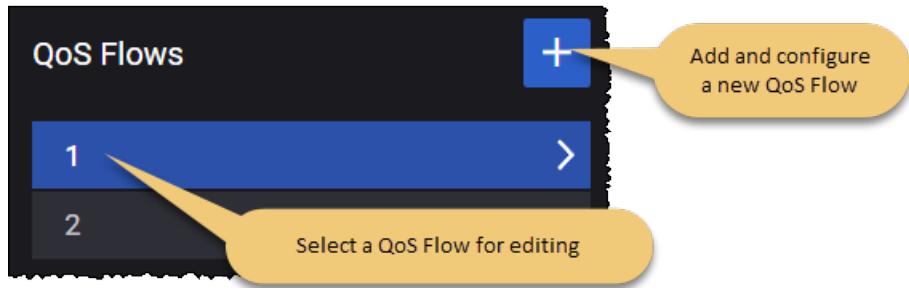
The profiles that you add will be available when managing agents from the [Network Management on page 81](#) window.

QoS Flows panel

The QoS model is based on QoS Flows. A QoS Flow is the finest level of granularity for QoS forwarding treatment in the system. All traffic mapped to the same QoS Flow receives the same forwarding treatment.

Accessing the configuration settings:

To access the QoS Flows configuration settings, select **QoS Flows** from the the **Global Settings** panel. Cu Isolation opens the **QoS Flows** panel from which you can add and edit QoS Flow definitions:



These QoS Flow configurations become immediately available for selection by other nodes in the test configuration. The properties for a QoS Flow are organized into the following groups of configuration settings:

QoS Flows configuration settings	63
QoS Flow Packet Filter configuration settings	67
QoS Flow Max Packet Loss Rate settings	68
QoS Flow ARP configuration settings	68
QoS Flow MBR configuration settings	69
QoS Flow GBR configuration settings	69

QoS Flows configuration settings

You create and manage QoS Flows for your test network in the **Global Settings** section of the **Test Overview**. The **QoS Flows** panel contains the configuration settings for an individual QoS Flow. In this panel, you can:

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

The **QoS Flow** settings are described in the table that follows.

Setting	Description
<i>QoS Flow:</i>	
Is Default	Enable this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule

Setting	Description
	will be associated with a QoS Flow.
Is Delay Critical	If enabled, it ensures that data packets are delivered within a very short time frame, minimizing latency. This is crucial for applications that need real-time or near-real-time communication.
Type	<p>IMPORTANT This parameter is available only if the Is Default option is not selected.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • Data - PCF/PCRF is capable by itself to generate Packet filters for this flow/bearer. This type of flow/bearer is used for non-Voice or non-Video traffic. • Audio - PCF/PCRF needs information related to this flow/bearer from CSCF. • Video - PCF/PCRF needs information related to this flow/bearer from CSCF.
Network Initiated Flow	<p>IMPORTANT This parameter is available only if the Is Default option is not selected.</p> <p>Select the associated check box to enable this option.</p> <p>The following fields are displayed:</p> <ul style="list-style-type: none"> • <i>Delay After Initial Registration (s)</i> - set the value for this parameter. • <i>Interval between Create and Delete (s)</i> - set the value for this parameter. • <i>Iterations</i> - set the value for this parameter.
QFI	Enter a QoS Flow Identifier (QFI) for this QoS Flow. This identifier will be used to uniquely identify a QoS Flow in the 5G System. All User Plane traffic with the same QFI within a PDU Session receives the same traffic forwarding treatment. The QFI is carried in an encapsulation header on the N3 and N9 reference points.
5QI	<p>Specify the 5QI value (decimal number).</p> <p>5G QoS Identifier (5QI) is a scalar that is used as a reference to 5G QoS characteristics defined in TS 23.501, clause 5.7.4. These are access node-specific parameters that control QoS forwarding treatment for the QoS Flow (such as scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, among others). Standardized 5QI values have a one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in TS 23.501, table 5.7.4-1.</p>
5QI Priority Level	Specify the 5QI Priority Level for this QoS Profile. 5QI Priority Level is a Policy Control parameter that accepts values from 1 through 127 (where 1 is the highest priority). It indicates a priority in scheduling resources among QoS Flows.
Resource Type	Select the type of resource that the QoS Flow requires: Guaranteed Bit Rate (GBR), Non-Guaranteed Bit Rate, or Delay Critical GBR. The Resource Type determines whether or not dedicated network resources related to a QoS Flow-level Guaranteed Flow Bit Rate (GFBR) value are permanently allocated to the

Setting	Description
	flow.
Averaging Window	Specify the <i>Averaging window</i> value for this 5GI. Each GBR QoS Flow is associated with an <i>Averaging window</i> . It represents the time duration (specified in milliseconds) over which the GFBR and MFBR are calculated.
QoS Rule Precedence	<p>Specify the desired QoS Rule Precedence value for this QFI.</p> <p>The QoS rule precedence value (and the PDR precedence value) determine the order in which a QoS rule or a PDR, respectively, will be evaluated. The evaluation of the QoS rules or PDRs is performed in increasing order of their precedence value.</p>
Packet Delay Budget	The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the UE and the PCEF. For a given QCI, the value of the PDB is the same in uplink and downlink. The purpose of the PDB is to support the configuration of scheduling and link layer functions.
Packet Error Rate	The Packet Error Rate (PER) defines the upper bound for the rate of PDUs (IP packets) that have been processed by the sender of a link layer protocol but are not successfully delivered by the corresponding receiver to the upper layer. It defines an upper bound for the rate of non-congestion related packet losses.
Max Data Burst	The Maximum Data Burst Volume is the amount of data which the RAN is expected to deliver within the part of the Packet Delay Budget allocated to the link between the UE and the radio base station.
QoS Reference	<p>This option is used on the PCF node to identify a particular PCC Rule when QoS reference information is received from the NEF on N33 interface.</p> <p>NOTE QoS Reference is supported only when Technical Spec Version is R16 or higher.</p>
Notification Control	Enable or disable the Notification Control parameter. When enabled, it indicates whether notifications are requested from the RAN when the GFBR can no longer be fulfilled for a QoS Flow during the QoS Flow's lifetime.
Segregation	Enable this option if the Segregation indication is to be included in a UE initiated PDU Session Modification procedure. The Segregation indication is included when the UE requests that the network bind the applicable SDF(s) on a distinct and dedicated QoS Flow.
Use Match-all Packet Filter	<p>IMPORTANT This is available if Is Default option is enabled.</p> <p>If this option is not enabled, a new Packet Filter List option appears and custom packet filter can be configured.</p>
EPS Bearer Identifier	The EBI for the bearer associated with this QoS flow.
PCC Rule	Set a value for this parameter.

Setting	Description
Name	
Is Predefined Rule	Select the check box to enable this option.
Application Identifier	Set the application identifier value.
Send QoS Rule Precedence when Application identifier is configured	If needed, enable this option.
Move to Secondary Node	If needed, enable this option. This option is part of the Option 3x and Dual Connectivity NR feature.
Packet Filter List	<p>IMPORTANT This is available if Use Match-all Packet Filter option is not selected.</p> <p>Refer to the following topic for a description of the Packet Filter configuration settings: QoS Flow Packet Filter configuration settings.</p>
Max Packet Loss Rate	Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: QoS Flow Maximum Packet Loss configuration settings .
ARP	Refer to the following topic for a description of the ARP configuration settings: QoS Flow ARP configuration settings .
MBR	Refer to the following topic for a description of the MBR configuration settings: QoS Flow MBR configuration settings .
GBR	Refer to the following topic for a description of the GBR configuration settings: QoS Flow GBR configuration settings .

QoS Flow Packet Filter configuration settings

A Packet Filter Set is used in the definition of QoS rules or packet detection rules (PDRs) to identify one or more packet flows for filtering.

You use the settings in the QoS Flow **Packet Filter List** panel to configure the packet filters associated with the current flow. You access this panel from the QoS Flow panel:



The **Packet Filter** settings are described in the following table.

Setting	Description
	Select the Delete Packet Filter button to delete this Packet Filter from the test configuration.
Direction	Select the direction of the data flow on which the filter is applied from the drop-down list: Uplink, Downlink, or Bidirectional.
IPv4 Remote Address and Subnet Mask	The IPv4 address of the remote node plus the subnet mask. If the <i>Direction</i> is Uplink, then this IP address is the destination IP. If the <i>Direction</i> is Downlink, then this IP address is the source IP.
IPv6 Remote Address and Prefix Length	The IPv6 address for the remote node, expressed in CIDR notation (for example: 2001:db8::/32). If the <i>Direction</i> is Uplink, then this IP address is the destination IP. If the <i>Direction</i> is Downlink, then this IP address is the source IP.
Protocol Identifier or Next Header	The Protocol ID of either the protocol above IP in the stack or the next header type. Examples: UDP, TCP, ESP.
Single Local Port	The local port number, if the filter specifies a single port.
Single Remote Port	The remote port number, if the filter specifies a single port.
Local Port Range	The low and high limits for local port range.
Remote Port Range	The low and high limits for remote port range.

Setting	Description
Security Parameter Index	The Security Parameters Index (SPI) for this packet filter. The SPI is a pointer that references the session key and algorithms used to protect the data being transported.
Type Of Service or Traffic Class	The IPv4 Type of Service (TOS) or the IPv6 traffic class.
Flow Label	The IPv6 Flow Label. This refers to the 20-bit Flow Label field in the IPv6 header.

QoS Flow Max Packet Loss Rate settings

The settings establish the uplink and downlink maximum packet loss that is permitted for the QoS flow.

Setting	Description
<i>Maximum Packet Loss Rate:</i>	
Uplink	The maximum uplink packet loss rate (packets per second) that is permitted for the QoS Flow.
Downlink	The maximum downlink packet loss rate (packets per second) that is permitted for the QoS Flow.

QoS Flow ARP configuration settings

The Allocation and Retention Priority (ARP) settings specify the priority level, preemption capability, and preemption vulnerability of a resource request. It is used to determine whether a new QoS Flow should be accepted or rejected—and to determine whether an existing QoS Flow can be preempted by another QoS Flow—in response to resource limitations.

The **QoS Flow ARP** settings are described in the table that follows.

Setting	Description
<i>ARP:</i>	
ARP Priority Level	Specify the ARP priority level. The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.
Preemption Capability	Enable this option if the packets in this QoS Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.

Setting	Description
Preemption Vulnerability	Enable this option if the packets in this QoS Flow are candidates for being preempted by other flows. When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.

QoS Flow MBR configuration settings

MBR indicates the maximum bit rates allowed for service data flows that are mapped to this QoS flow. Separate MBR values are configured for uplink and downlink traffic.

The **QoS Flow MBR** settings are described in the table that follows.

Setting	Description
<i>MBR:</i>	
Uplink Bitrate Unit	Select the uplink bitrate unit from the drop-down list.
Uplink Bitrate Value	Set the maximum bit rate value for uplink traffic.
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set the maximum bit rate value for downlink traffic.

QoS Flow GBR configuration settings

GBR indicates the guaranteed bit rates for service data flows that are mapped to this QoS flow. Separate GBR values are configured for uplink and downlink traffic.

The **QoS Flow GBR** settings are described in the table that follows.

Setting	Description
<i>GBR:</i>	
Uplink Bitrate Unit	Select the uplink bitrate unit from the drop-down list.
Uplink Bitrate Value	Set the guaranteed bit rate value for uplink traffic.
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set the guaranteed bit rate value for downlink traffic.

DRBs

A data radio bearer (DRB) is a logical communication channel that facilitates data transmission between the User Equipment (UE) (such as your smartphone) and the Evolved Packet Core (EPC) network. It serves as a bi-directional data transmission path that carries user data between the UE and the EPC.

The DRBs' main roles cover:

- Transporting User Data, being responsible for transporting actual user-generated information, including voice calls, video streams, and internet data.
- Quality of Service (QoS), where they play a pivotal role in ensuring that user data is transmitted efficiently while adhering to specific quality of service requirements.

Setting	Description
<i>DRBs</i>	
	Click the Add DRB button to add a new data radio bearer to your test configuration.
<i>DRB</i>	
	Click the Delete DRB button to remove the selected data radio bearer from your test configuration.
DRB ID	The unique identifier of this radio bearer.
RLC Mode	Select the RLC Mode to identify the NR RLC Mode. <ul style="list-style-type: none"> • TR (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)
PDCP:	<i>Select to configure the 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.
SDAP:	<i>Select to configure the Service Data Adaptation Protocol.</i>
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).
Downlink Header	Enable this option if an SDAP header should be included for this DRB for Downlink Data.

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, Cu Isolation 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.

Override Milenage Constants

The following table describes the settings required to override the milenage constants.

Setting	Description
<i>Override Milenage Constants</i>	<i>Enable this option to override the milenage constants.</i> <i>The following fields are available only when this option is enabled.</i>
C1	Set the C1 value (string type). Default value: 00000000000000000000000000000000 .
R1	Set the R1 value (integer type). Default value: 64 .
C2	Set the C2 value (string type). Default value: 00000000000000000000000000000001 .
R2	Set the R1 value (integer type). Default value: 0 .
C3	Set the C3 value (string type). Default value: 00000000000000000000000000000002 .
R3	Set the R3 value (integer type). Default value: 32 .
C4	Set the C4 value (string type).

Setting	Description
	Default value: 00000000000000000000000000000004.
R4	Set the R4 value (integer type). Default value: 64.
C5	Set the C5 value (string type). Default value: 00000000000000000000000000000008.
R5	Set the R5 value (integer type). Default value: 96.

Customer Parameters

The section allows you to enable and use custom parameters. When this setting is enabled, you can use the **Custom Parameter** field to add the custom parameters.

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 Certificate 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 your test configuration.

Global Playlists

The following table describes the settings required to define the global playlists.

Setting	Description
<i>Global Playlists:</i>	

Setting	Description
	Select the Add Global Playlist button to add a new playlist to your test configuration.
<i>Impairment Profile:</i>	
	Select the Delete Global Playlist button to remove the playlist from your test configuration.
Name	Each playlist profile is uniquely identified by a name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Playlist file (.csv)	It allows you to add a custom playlist, using the Upload button. To remove the file, select the Clear button.

CHAPTER 6

Assign and manage agents

A Cu Isolation *agent* is the virtual machine 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	75
Assigning agents to nodes	76
Agent management	78
Network Management	81
Distribution Mode feature	82

About traffic agents

Cu Isolation tests require the use of *agents* to generate traffic for both DU-UP/CU-UP (user plane) and DU-CP/CU-CP (control plane), and/or Core. 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

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 Cu Isolation. 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 78 for instructions.

Assigning agents to nodes

You cannot run a Cu Isolation 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.

Cu Isolation 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, KIN, and Passthrough Device **Connections** as 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	Hover over the Owner icon to see the current agent ownership and status, which

Column	Description
	<p>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. Refer to About traffic agents on page 75 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> <p>NOTE For the Cu Isolation nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.</p>

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 Cu Isolation 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 80](#)

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 Cu Isolation. 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 number of cores.
Last Run	Displays the nodes that were last run on the agent.

Column	Description
Data	
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.

The screenshot shows the Network Management interface. At the top, there's a header with 'START TEST' and 'Test is not started'. Below this is a navigation bar with 'TEST OVERVIEW' (which is currently active, indicated by a blue underline), 'AGENTS ASSIGNMENT', and 'NETWORK MANAGEMENT'. Under 'TEST OVERVIEW', there's a 'Test Summary' section with 'DU Count' (2) and 'Cell C' (2). In the 'AGENTS ASSIGNMENT' section, it says '1 agent selected' and has a 'Filter agents' button. The main area is a table with columns: 'Order', 'Agent', 'Tags', and 'Impairment Profile'. The first row shows 'Order' 1, 'Agent' 10.39.34.51, 'Tags' IxStack: ON(1), Raw Socke... (1), version: o... (1), and 'Impairment Profile' None. There are also dropdown menus for 'Order' (set to 1) and 'Agent' (set to 10.39.34.51).

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 Cu Isolation. 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 79 for more details. <p>Each tag indicates the number of agents to which it was associated.</p>
Impairment profile	Allows you to 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 IxStack: On/Off system tag.</p>
SRIoV	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).
Traffic Capture	This option allows you to enable or disable traffic capture on all or specific interfaces, based on your test configuration.
Entity	Displays the nodes on which the agent has been assigned. When hovering over the node, it displays the node's interface names.

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.

Distribution Mode feature

Distribution Modes for Nodes

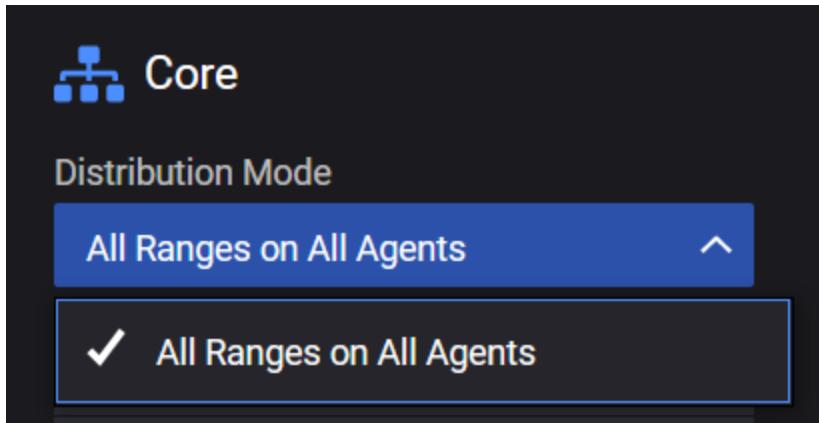
For convenience, you are now able to see or select (if available), the way node ranges are distributed on agents. The **Distribution Mode** parameter is available even if no agents are assigned, but its value can change when assigning multiple agents and/or when adding multiple ranges.

When opening a node for configuration, the **Distribution Mode** parameter is displayed and options such as the following can be selected or observed:

Distribution Mode	Description/Example
All Ranges on All Agents	<p>All ranges will be distributed on all agents and the IP addresses will be incremented.</p> <p>For example, in a test with 2 agents and 3 ranges:</p> <ul style="list-style-type: none"> • range1 on agent1 and agent2

Distribution Mode	Description/Example
	<ul style="list-style-type: none"> range2 on agent1 and agent2 range3 on agent1 and agent2
Round Robin Ranges on Agents	<p>Each range will be configured on one agent. One agent can have multiple ranges configured.</p> <p>For example, in a test with 2 agents and 3 ranges:</p> <ul style="list-style-type: none"> range1 on agent1 range2 on agent2 range3 on agent1.
One Range on All Agents	<p>One range will be configured on all assigned agents. For example, in a test with 2 agents and 1 range:</p> <ul style="list-style-type: none"> range 1 on agent 1 and 2.
All Ranges on One Agent	This mode allows only one agent in the assignment.
One Range on One Agent	In this mode each range requires a different agent.

For more details, refer to each node for the available distribution mode.

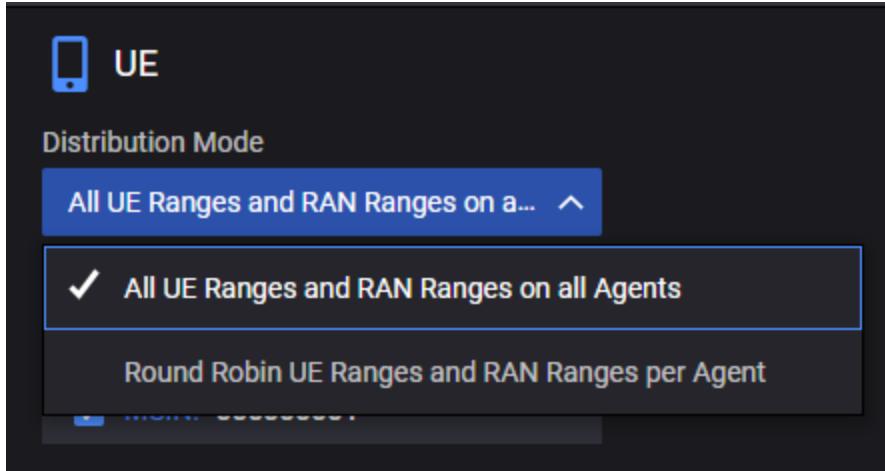


UE-RAN Distribution Modes (configurable on UE box)

Similarly to node distribution, if multiple agents are assigned to RAN, the user can change the distribution mode from the UE box. Based on how many agents were assigned and how many UE ranges are available, the configuration page will display the **Distribution Mode** parameter and the following options can be selected from the drop-down:

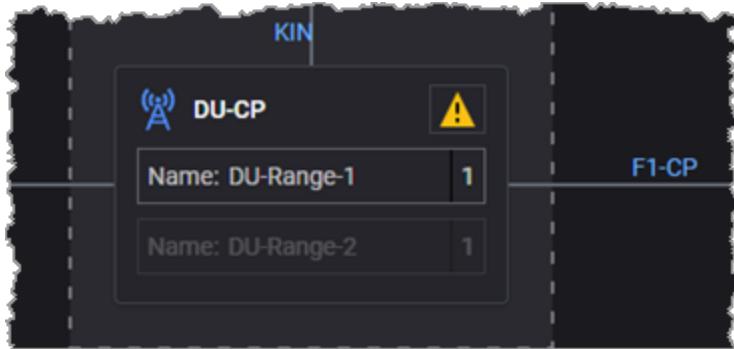
Distribution Mode	Description/Example
All UE Ranges and RAN Ranges on All Agents	<p>For example, for a test with 2 agents and 2 UE ranges and 2 RAN ranges:</p> <ul style="list-style-type: none"> UE range1 and UE range2 and their parent ranges as well

Distribution Mode	Description/Example
	as all RAN ranges part of Mobility Path and Secondary RAN ranges will be distributed to both agent1 and agent2
Round Robin UE Ranges and RAN Ranges per Agent	For example, if UE range1 is distributed to agent1, parent RAN range as well as all RAN ranges part of the Mobility Path (visited gNB/eNB ranges), and the Secondary RAN ranges will also be distributed on agent1.



CHAPTER 7

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 Cu Isolation 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	86
DU-CP RANGE panel	87
Cells settings	89
Measurement Timing Configuration	91
F1-CP Interface Settings	92
DU-PROCEDURE RANGE panel	99

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 ...



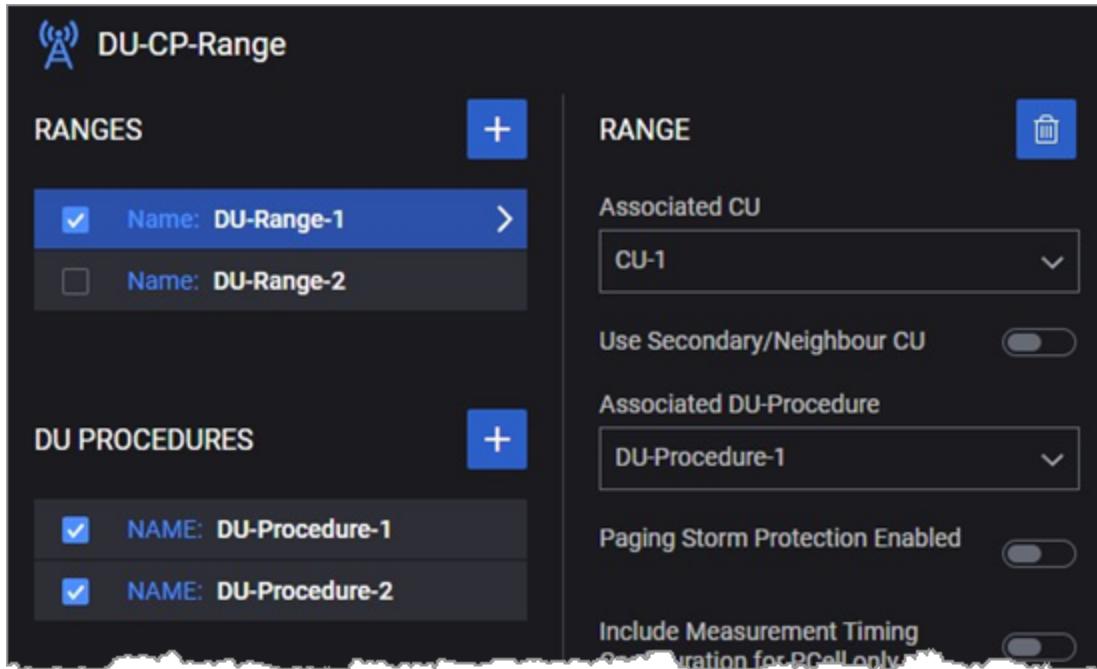
DU Procedure ranges

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 described in [DU-CP RANGE panel](#)).

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, Cu Isolation 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.

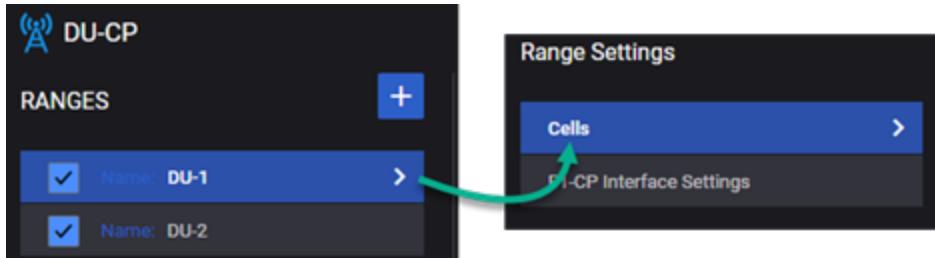
The following table describes the available settings that are required for each DU-CP range.

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 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 CU.</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 CU.
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 CU.				

Setting	Description
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 .
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.
Use Serving Cell Config Common in SB1	If enabled, it includes cell configuration parameters in the SIB message in F1 setup request procedure.
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 .
F1-CP Interface	Refer to F1-CP Interface Settings .

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](#)
- [NSSAI](#)
- [Cells Settings](#)

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 (PCI)	The NR Cell Global Identifier (NRCGI) for this Cu Isolation range.
Cell ID (PCI) Increment	Enter the value by which Cu Isolation will increment each <i>Cell ID</i> if the <i>Cell Count</i> is greater than 1.
Cell (PCI) 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 <u>Measurement Timing Configuration</u> 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

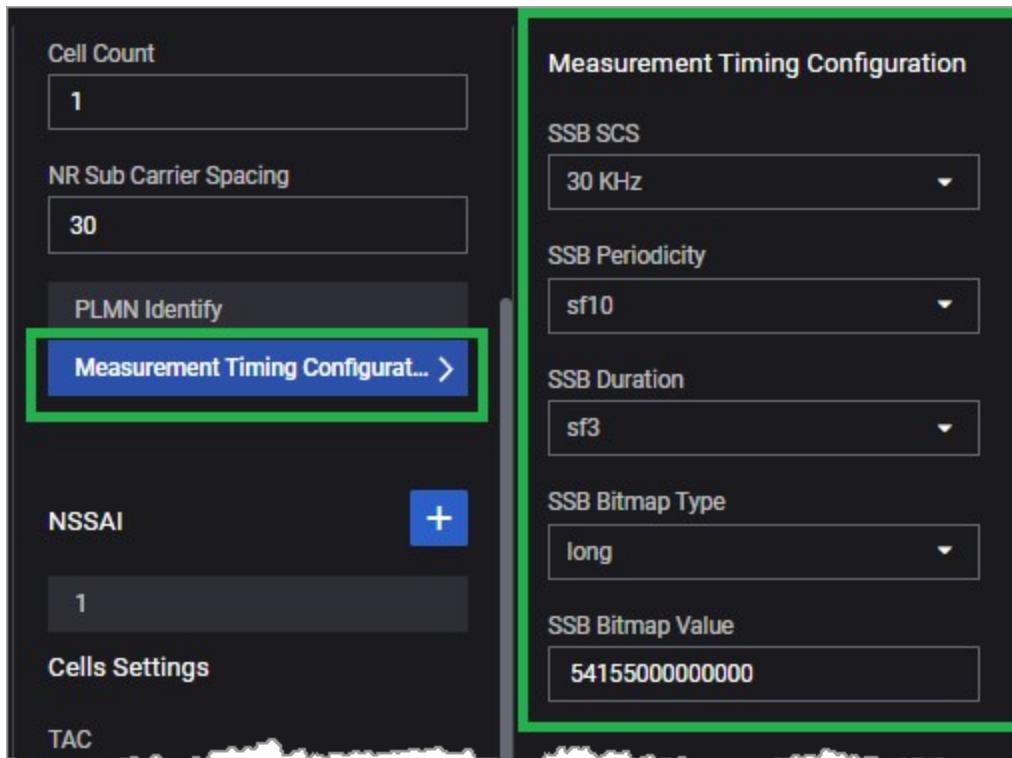
Each DU-CP range requires configuration of a group of **Cells Settings** settings, which are described in the following table. These value are used by each of the cells defined in this DU-CP range.

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. The default value is 11, the minimum is 1, and the maximum is 261. These correspond to the n1, n2, ..., n261 band

Setting	Description
	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.

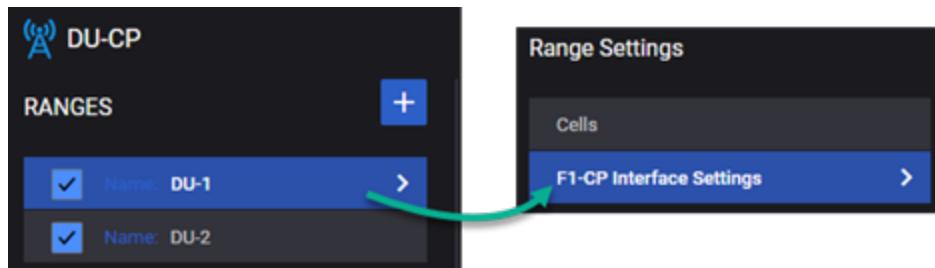
The following table describes the configuration settings.

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](#)
- [Connectivity Settings](#)

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 Cu Isolation 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](#)
- [VLAN settings](#)
- [IPsec settings](#)

F1C IP Connectivity Settings

These settings specify the F1-CP IP settings.

Setting	Description
IP Address	Enter the IP address that the first Cu Isolation 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 RANGE</i> 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.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the 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, Cu Isolation 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.
Inner IP Type	Select the IP type: IPv4 or IPv6.
<i>IP:</i>	
IP Address	The IP address of the F1-C interface on the DU range.
IP Address Increment	The IP address prefix assigned to this interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
IP Prefix Length	Set the IP address increment value.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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>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 Cu Isolation Global settings. Refer to CA Certificates Settings for instructions.

Setting	Description
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	Use the uploaded certificate and key file for all test instances of this configuration.
<i>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</p>

Setting	Description
	group 1 is a 768-bit group and DH group 2 is a 1024-bit group.
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>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 <i>-GCM</i> 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>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

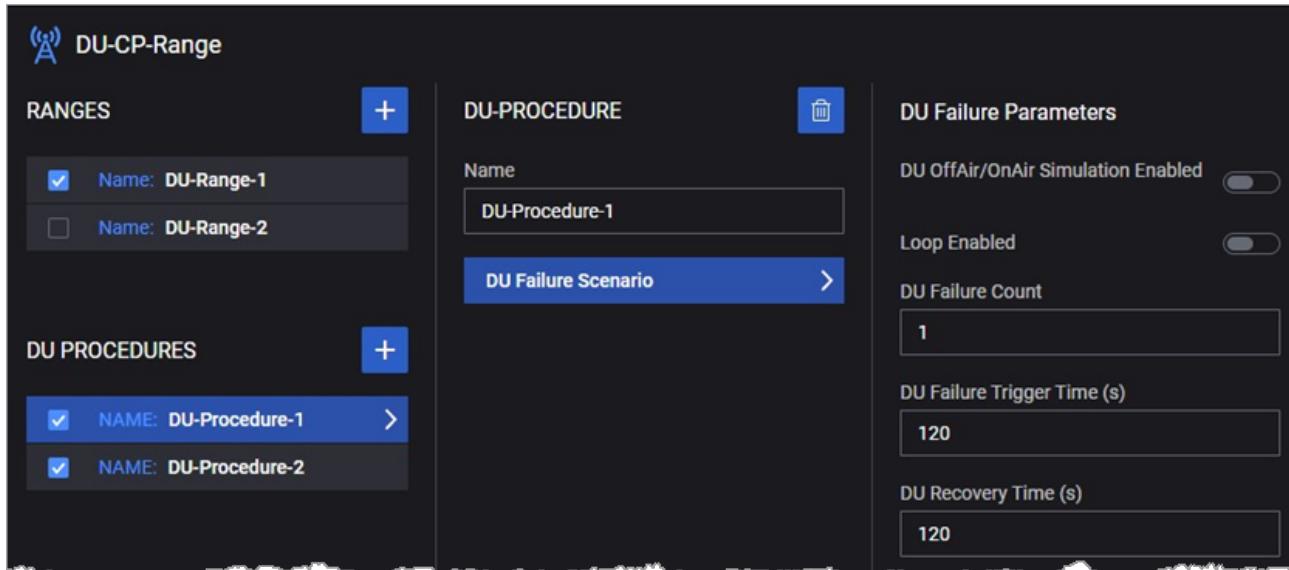
Setting	Description
	<p>and inserts the gateway address into the Identification Data field as a single four-octet IPv4 address.</p> <ul style="list-style-type: none"> • ID_FQDN: Sets the Identification Type field to 2 and inserts the gateway address into the Identification Data field as a fully-qualified 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>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	Specifies the Phase 1 Security Association (SA) lifetime, in seconds.

Setting	Description
(s)	The valid range of values is 0 through 31,557,600.
IKE Phase 2 (ESP) Lifetime (s)	Specifies the Phase 2 Security Association (SA) lifetime, in seconds. The valid range of values is 0 through 31,557,600.
DPD Interval (s)	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. 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: <ul style="list-style-type: none"> • DPD HELLO • DPD HELLO ACK 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.
IKE Retry Count	Enter the number of retries for IKE SA INIT or IKE AUTH request messages. 0 means that retry is disabled.
IKE Retry Timeout (s)	This parameter determines how long the system waits before retransmitting an IKE message if a response is not received.

DU-PROCEDURE RANGE panel

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

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



DU-PROCEDURE range panel settings

When you select a DU-PROCEDURE range from the **DU-CP Range** panel, Cu Isolation 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 Cu Isolation.
DU Failure Scenario	Select to open the DU Failure Parameters panel.

DU Failure Parameters

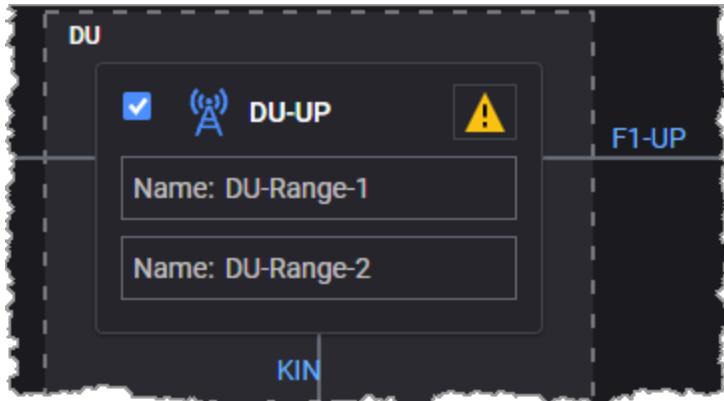
The following table describes the DU Failure Parameters.

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 8

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 Cu Isolation 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	102
DU-UP Range panel	103

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.

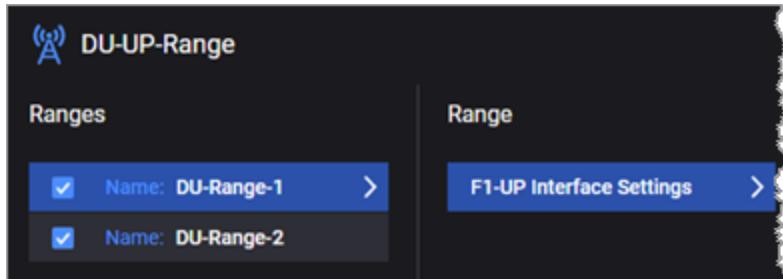
For example ...



Cu Isolation manages DU-UPCU-UP ranges as follows:

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

DU-UP Range panel



When you select a DU-UP range from the **DU-UP Ranges** panel, Cu Isolation 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](#)
- [Connectivity Settings](#)

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 Cu Isolation to include sequence numbers in T-PDUs.

Connectivity Settings

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

- [IP Settings](#)
- [MAC Settings](#)
- [VLAN settings](#)
- [IPsec settings](#)

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	Enable to use the UDP checksum for this F1-UP IP interface.
Gateway Address	This DU-UP node's gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).

MAC Settings

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

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

Setting	Description
VLAN	
Inner VLAN	When <i>Outer VLAN</i> is enabled, Cu Isolation 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.
Inner IP Type	Select the IP type: IPv4 or IPv6.
<i>IP:</i>	
IP Address	The IP address of the F1-U interface on the DU range.
IP Address Increment	The IP address prefix assigned to this interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
IP Prefix Length	Set the IP address increment value.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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>Authentication settings:</i>	
Authentication Method	Select the authentication method to use in this configuration. The options are: <ul style="list-style-type: none"> Certificates: Use CA certificates for authentication.

Setting	Description
	<ul style="list-style-type: none"> • 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 Cu Isolation Global settings. Refer to CA Certificates Settings 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.
Use Same Certificate and Private Key for all Instances	Use the uploaded certificate and key file for all test instances of this configuration.
<i>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</p>

Setting	Description
	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.
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>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 <i>-GCM</i> 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>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.

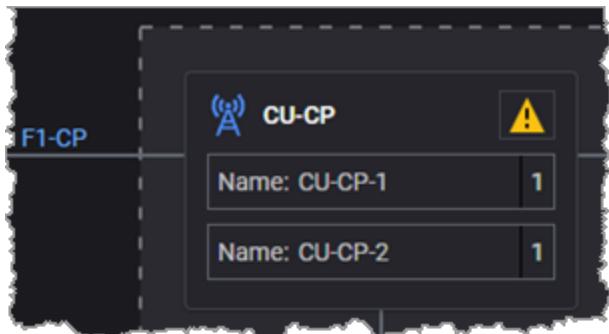
Setting	Description
	<ul style="list-style-type: none"> • ID_FQDN: Sets the Identification Type field to 2 and inserts the gateway address into the Identification Data field as a fully-qualified domain name string. For example, "foo.bar.com". • ID_USER_FQDN: Sets the Identification Type field to 3 and 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	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. 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</p>

Setting	Description
	<p>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>
IKE Retry Count	Enter the number of retries for IKE SA INIT or IKE AUTH request messages. 0 means that retry is disabled.
IKE Retry Timeout (s)	This parameter determines how long the system waits before retransmitting an IKE message if a response is not received.

CHAPTER 9

gNB CU-CP configuration settings

The gNB Centralized Unit (gNB-CU) is a logical node hosting PDCP and SDAP layers of the gNB. One gNB-CU supports one or multiple cells, and it terminates the F1 interface connected with the gNB-DU.



In the Cu Isolation test topology, the gNB-CU is logically structured as two entities:

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

The CU-CP/CU-UP will act as a DUT when the Device Under Test flag is enabled for these nodes.

Chapter contents:

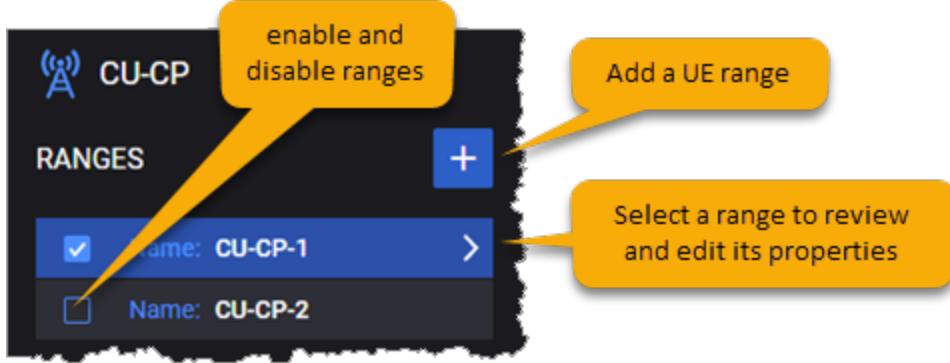
CU-CP Ranges panel	111
CU-CP Range settings	112
Settings panel	114
Cells settings	116
F1-CP Interface Settings	119
X2-C Interface Settings	119
Xn-C Interface Settings	120
CU-CP KIN Interface settings	121

CU-CP Ranges panel

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

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

For example:



Refer to [CU-CP Range settings](#) for a description of the CU-CP range settings.

CU-CP Range settings

Each CU-CP Range is identified by a unique name and can be enabled or disable for a given test run.

The following table describes the Range Settings that you configure for each CU-CP range.

Settings	Description
	Delete the selected CU-CP range from the test configuration.
Device Under Test	Enable this option if this node is the DUT in this configuration settings. When enabled, it will also allow the configuration of the CU-CP identification settings, as described in the following rows. When this option is not enabled, the application will simulate the node's functionality (if it is selected in the Topology window), the CU-CP and CU-UP against DU, respectively.
Name	<p>NOTE This parameter appears only if Device Under Test is enabled for this range.</p> <p>Keysight Open RAN Simulators, Cloud Edition 5.0 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.</p>

Settings	Description
CU ID	<p>NOTE This parameter appears only if Device Under Test is enabled for this range.</p> <p>The gNB-CU Identifier (which is part of the NR Cell Identity). The valid value range is from 0 to 4,294,967,295.</p>
CU ID Length	<p>NOTE This parameter appears only if Device Under Test is enabled for this range.</p> <p>The length (number of bits) of the CU ID. The ID can be configured to use between 22 bits and 32 bits.</p>
Associated AMF	Select a previously-configured AMF to associate with this CU-CP range.
<i>Range Settings:</i>	
Settings	<p>Each CU-CP range requires the configuration of an associated Node Settings which are described in section Settings panel.</p> <p>NOTE If Device Under Test is enabled, this section will not be visible.</p>
Cells	<p>Each CU-CP range requires the configuration of an associated Cells which are described in section Cells settings.</p> <p>NOTE If Device Under Test is enabled, this section will not be visible.</p>
F1 Interface Settings	Each CU-CP range requires the configuration of F1 interface settings, through which CU-CP instance interacts with gNB-DU-CP Node. These settings are described in section F1-CP Interface Settings .
X2C Interface Settings	Each CU-CP range requires the configuration of X2-C interface, which carries signaling packets between RAN nodes in non-standalone (NSA) operations. These settings are described in section X2-C Interface Settings .
Xn-C Interface Settings	<p>Each CU-CP range requires the configuration of Xn, which 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.</p> <p>These settings are described in section Xn-C Interface Settings.</p>
KIN Interface Settings	<p>Each CU-CP range requires the configuration of KIN interface settings, through which CU-CP node and CU-UP nodes communicate. This interface is an internal interface (not exposed to DUT) and suggested to be configured through an internal network within CUSIM. These settings are described in section CU-UP KIN Interface Settings.</p> <p>NOTE If Device Under Test is enabled, this section will not be visible.</p>

Settings panel

The Settings panel provides access to the CU-CP node settings described in the following table.

Settings	Description
Requests cells activation at F1 Setup	If this checkbox is enabled, CU-CP requests the gNB-DU-CP to activate cells via F1 Setup Response message, then gNB-DU-CP will initiate gNB-DU Configuration Update procedure for cell activation. If this checkbox is not enabled, gNB-CU initiates gNB-CU Configuration Update procedure for cell activation after F1 Setup procedure.
Name	The name uniquely identifies the CU-CP. You can accept the value provided by CUSIM or overwrite it with your own value.
CU ID	Enter the gNB-CU Identifier for this CU-CP range. It can be configured to use between 22 bits and 32 bits. The valid value range is 0 - 4,294,967,295.
CU ID Length	The number of bits (from NRCGI) to use for gNB-CU Identifier. (The number of bits to use for CU ID is a vendor decision.)
F1 Setup Wait Time	This parameter defines the value of the "Time to Wait" IE set by the gNB-CU in the F1 Setup Failure message.
Default DRX Paging Cycle	Select the desired Discontinuous Reception (DRX) Paging Cycle from the drop-down list. This value indicates the DRX periods within each paging cycle during which the UE will monitor the paging channel.
Activity Notification Level	Select the desired Activity Notification that will be performed for this CU-UP node: DRB, PDU Session, or UE. Refer to TS 38-463 for detailed information.
Disable NRUP	Enable or disable NR user plane protocol. It is enabled in the CU by default. The NR user plane protocol, which is located in the User Plane of the Radio Network layer over the Xn, X2, or F1 interface, is used to convey control information related to the user data flow management of data radio bearers. In Cu Isolation, it is used by the CU to query the DU over the F1 interface and obtain parameter values such as data rate and buffer size.
PLMN Identity	Refer to PLMN Identity on the next page below.
SCTP Buffers	Refer to SCTP Buffers on the next page below.
UDP Buffers	Refer to UDP Buffers on the next page below.

PLMN Identity

Configure the values in the following table to construct the PLMN Identify value to include in CU-CP messages. The PLMN is the concatenation of the MCC and MNC.

Setting	Description
PLMN MCC	The PLMN's MCC value.
PLMN MNC	The PLMN's MNC value.

SCTP Buffers

The F1-C signaling bearer uses SCTP (Stream Control Transmission Protocol) for reliable transport of messages. Configure the following SCTP buffers for CU-CP messages.

Setting	Description
Transmit (bytes)	The number of bytes for the SCTP transmit buffer.
Receive (bytes)	The number of bytes for the SCTP receive buffer.

UDP Buffers

Configure the UDP buffers for CU-CP messages.

Setting	Description
Transmit (bytes)	The number of bytes for the UDP transmit buffer.
Receive (bytes)	The number of bytes for the UDP receive buffer.

Cells settings

Each CU-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](#)
- [NSSAI](#)
- [SIB](#)

Cells

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

Settings	Description
Cell ID	Cell Identifier for this range. The NR Cell Identifier (NCI) is calculated using CU ID, and CU ID length: NCI (36 bits) = gNB-CU Identity (CU ID Length) + Cell ID (CU ID Length) .
Cell ID Increment	Enter the value by which CuSIM will increment each Cell ID if the Cell Count is greater than 1.
Cell Count	If you want to create multiple cells for this cell range, enter the desired number in this field.
Use Neighbor Cell	If enabled, then the Neighbor Cell will be used for mobility.
Neighbor Cell	<p>NOTE This parameter appears only if Use Neighbor Cell is enabled.</p> <p>Assign the neighbor cell to be used for mobility.</p>
ARFCN	Enter the desired downlink New Radio Absolute Radio Frequency Channel Number.
SSB Frequency	The Frequency referring to the position of resource element RE=#0 (subcarrier #0) of resource block RB#10 of the SS block. Used for Handover decision.
Subcarrier 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.
TAC	The unique identifier of the Tracking Area Code (TAC) to which this cell belongs in the 5G system.
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:

Settings	Description
	<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	Refer to NSSAI below below.
SIB	Refer to SIB on the facing page below.

NSSAI

Each CU-CP 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 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	<p>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:</p> <p>1 (eMBB) 2 (URLCC) 3 (MIoT)</p>
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.

SIB

If you would like CU-CP to send optional gNB-CU System Information Block (SIB) values with the F1 Setup Response message, you can configure them from the SIB panel.

Setting	Description
SIB Type	Enter the System Information Block Type: 2 for sibType2, 3 for sibType3, and so forth.
SIB Message	Enter the hex string bytes - RRC SIB Message Container (OCTET STRING).

F1-CP Interface Settings

Each **CU-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 grouped into **F1 Interface Settings** and **Connectivity Settings**.

F1 Settings

The F1 interface settings specify the F1 port number.

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.

Connectivity Settings

The connectivity settings comprise the interface's IP address and, optionally, outer and inner VLAN identifiers.

Setting	Description
<i>IP settings:</i>	
IP Address	Enter the IP address that the first CuSIM CU-CP node defined in this range will use to communicate with gNB-DU (DUT)
IP Prefix Length	The subnet prefix length associated with this CU-CP IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	This CU-CP node's gateway address.
<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 <i>Outer VLAN</i> is enabled, Cu Isolation 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 .

X2-C Interface Settings

You access the X2-C Interface Settings from a CU range panel ([CU-CP Range settings](#)). 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.
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](#) 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-CP Range settings](#)). 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.

CU-CP KIN Interface settings

The traffic agents of the CuSIM test nodes (CU-CP and CU-UP) communicate through an internal network called the Keysight Internal Network. The following table describes the settings for the KIN interface:

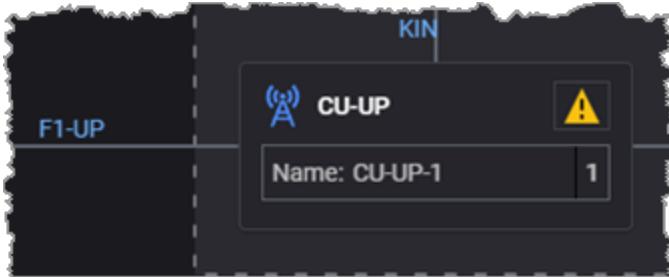
Settings	Description
IP Address	Enter the IP address of the KIN for this CU-CP node defined in this range will use to communicate with CU-UP node.
IP Prefix Length	The subnet prefix length associated with this KIN IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

CHAPTER 10

gNB CU-UP configuration settings

In the Cu Isolation test topology, the gNB-CU is logically structured as two entities:

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



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

Chapter contents:

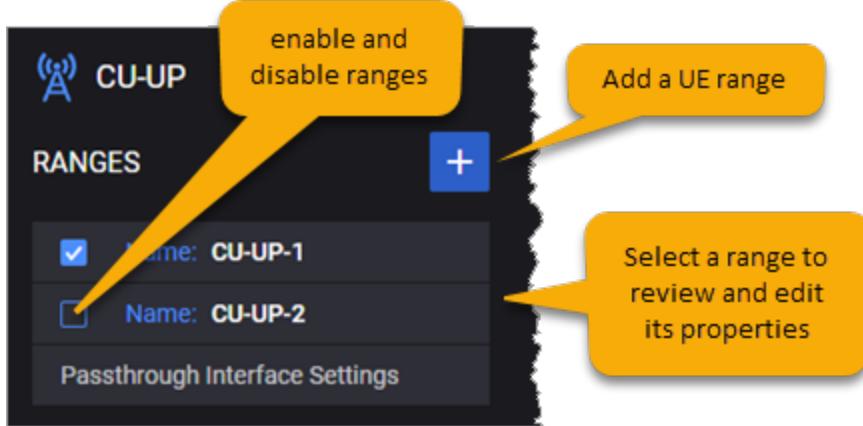
CU-UP RANGES panel	123
CU-UP Range settings	124
F1-UP settings	126
CU-UP KIN Interface Settings	128
Passthrough interface configuration	129

CU-UP RANGES panel

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

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

For example:

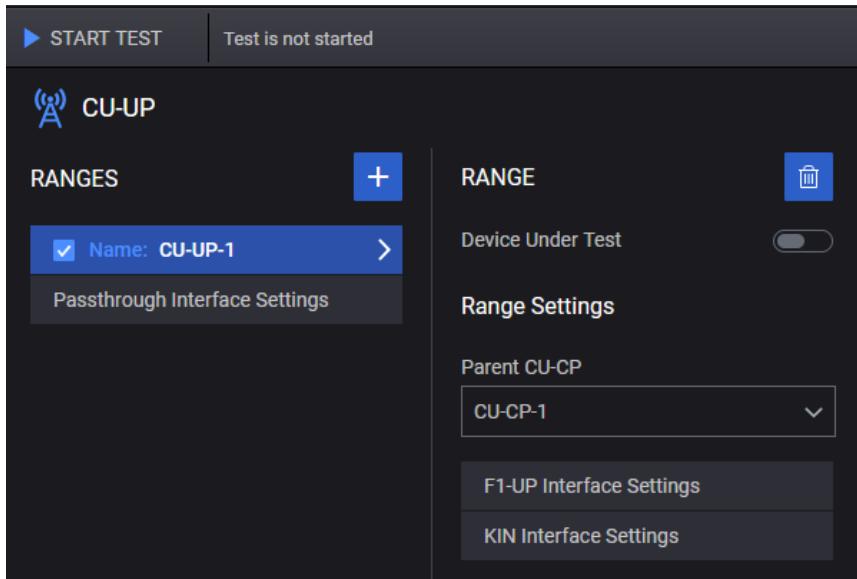


Refer to [CU-UP Range settings on the facing page](#) for a description of the CU-UP configuration settings.

CU-UP Range settings

When you select a CU-UP range from the **CU-UP Ranges** panel, Cu Isolation opens the **Range** panel, from which you configure the F1-UP interface settings and connectivity settings.

Each CU-UP Range is identified by a unique name and can be enabled or disable for a given test run.



The following table describes the Range Settings that you configure for each CU-CP range.

Settings	Description
	Delete the selected CU-UP range from the test configuration.
Device Under Test	Enable this option if this node is the DUT in this configuration settings. When this option is not enabled, the application will simulate the node's functionality (if it is selected in the Topology window). If enabled, this setting will allow only the configuration of the DUT F1-U setting.
Parent CU-CP	Select the parent CU-CP range. NOTE This parameter is not displayed if the Device Under Test is enabled.
<i>Range Settings:</i>	
DUT F1-U IP Address	NOTE This parameter appears only if Device Under Test is enabled for this range. If Device Under Test is enabled, configure the IP Address of the DUT F1-U interface. Else, CU-UP node will be emulated.
F1	Each CU-CP range requires the configuration of F1 interface settings, through which

Settings	Description
Interface Settings	<p>CU-CP instance interacts with gNB-DU-CP Node. These settings are described in section F1-UP settings.</p> <p>NOTE This section is not displayed if the Device Under Test is enabled.</p>
KIN Interface Settings	<p>Each CU-CP range requires the configuration of KIN interface settings, through which CU-CP node and CU-UP nodes communicates. This interface is an internal interface (not exposed to DUT) and suggested to be configured through an internal network within CUSIM. These settings are described in section CU-UP KIN Interface Settings.</p> <p>NOTE This section is not displayed if the Device Under Test is enabled.</p>

F1-UP settings

Each **CU-UP** range requires configuration of a group of **F1-CP Interface Settings**. These settings enable communication between the simulated CUs and your DUT (the DU). They are grouped into **F1 Interface Settings** and **Connectivity Settings**.

F1-UP Interface Settings

The F1 interface settings specify the F1 port number and the MTU value for this interface.

Setting	Description
F1-UP Port	The port to use for the F1 connection. The Cu Isolation default port number is 2152, which is the registered GTP-U protocol port. You can set this to a different value, if appropriate for your test requirements.
MTU	The desired Maximum Transmission Unit (MTU) for the F1 interface. The MTU specifies the largest packet that an Ethernet frame can carry.

Connectivity Settings

The F1-UP 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 F1-UP on this CU-CP node.
IP Count	The number of F1-UP interface IP addresses to create for this node.
IP Address Increment	The value (expressed in IP address notation) by which the IP addresses will be incremented.
IP Prefix Length	The subnet prefix length associated with this F1-UP IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	This CU-UP node's gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC settings:</i>	
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.
<i>VLAN settings:</i>	
Outer VLAN	<i>Enable this setting if you need VLAN IDs for your application traffic.</i>
VLAN ID	The VLAN identifier.
VLAN TPID	The VLAN Tag Protocol Identifier (TPID) is used in the VLAN Frame Extension (tag). This is an Ether Type value that identifies the protocol type of the tag.
Inner VLAN	<i>When Outer VLAN is enabled, Cu Isolation exposes the optional Inner VLAN setting. Enable this setting if you need inner VLAN IDs.</i>
VLAN ID	The VLAN identifier.
VLAN TPID	The VLAN Tag Protocol Identifier (TPID) is used in the VLAN Frame Extension (tag). This is an Ether Type value that identifies the protocol type of the tag.

CU-UP KIN Interface Settings

The traffic agents of the CuSIM test nodes (CU-CP and CU-UP) communicate through an internal network called the Keysight Internal Network. The following table describes the settings for the KIN interface settings for the CU-UP node.

Connectivity Settings

When you select KIN Interface Settings, Cu Isolation opens the **Connectivity Settings** panel, which contains an entry for each KIN (Keysight Internal Network) interface that you define.

Setting	Description
<i>IP settings:</i>	
IP Address	<p>Enter the IP address for the CU-UP node's KIN interface for this range. This is the user plane IP address for the simulated CUs. It can be on its own subnet, as it has no relationship with any other IP addresses in the test config.</p>
IP Prefix Length	The subnet prefix length associated with this CU-UP KIN IP interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

Passthrough interface configuration

If you need to use traffic types not provided by CuSIM, you can configure a Passthrough Interface at the CU-UP node and use Cu Isolation with external traffic servers. When Passthrough Interface is configured, Cu Isolation traffic configurations do not apply; instead, all traffic is routed to external servers through the configured passthrough interface.

Passthrough test requirements

The main requirements for Cu Isolation passthrough test include:

- Assigning agents to the CU-UP Passthrough Devices, on the Agents Assignment window. For example:
Refer to [Assign and manage agents on page 74](#) for more information.
- Configuring at least one L7 server in the Wireless IP Endpoints topology, which is one of the ORAN SIM CE Core topologies (refer to [Wireless IP Endpoints](#) for detailed information). Note that the Wireless IP Endpoints IP Client node is not required for CU-UP passthrough testing.
- Configuring a Passthrough Interface at the CU-UP node, as described below.

Passthrough interface settings

Select **Passthrough Interface Settings** from the CU-UP Ranges panel.

The passthrough interface—when configured—waits for an external traffic source. The following settings are required for the passthrough interface configuration.

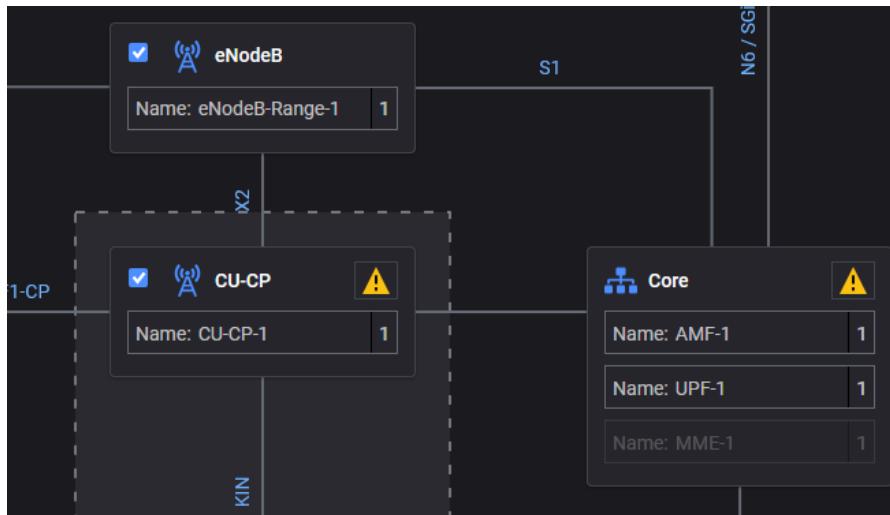
Setting	Description
<i>External L7 Servers:</i>	
	Click Add External L7 Server to add a new server.
address field	Enter the IP address of the external L7 server that you have configured for the test. In this example, a Data/Video server has been configured, and its range IP address is entered into the field:
	Delete an External L7 Server entry.
<i>Connectivity settings:</i>	
<i>IP:</i>	
IP Address	The IP address assigned as the external L7 Server's <i>Gateway Address</i> (in the Wireless IP Endpoints topology).
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

Setting	Description
Gateway Address	Enter a gateway address, if required. Otherwise, leave it set to 0.0.0.0.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
<i>MAC settings</i>	
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.
<i>VLAN settings:</i>	
Outer VLAN	<i>Enable this setting if you need VLAN IDs for your application traffic.</i>
VLAN ID	The VLAN identifier.
VLAN TPID	The VLAN Tag Protocol Identifier (TPID) is used in the VLAN Frame Extension (tag). This is an Ether Type value that identifies the protocol type of the tag.
Inner VLAN	<i>When Outer VLAN is enabled, Cu Isolation exposes the optional Inner VLAN setting. Enable this setting if you need inner VLAN IDs.</i>
VLAN ID	The VLAN identifier.
VLAN TPID	The VLAN Tag Protocol Identifier (TPID) is used in the VLAN Frame Extension (tag). This is an Ether Type value that identifies the protocol type of the tag.

CHAPTER 11

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, and the X2 interface connected with the gNB CU-CP.



This chapter describes the eNodeB settings.

Chapter contents:

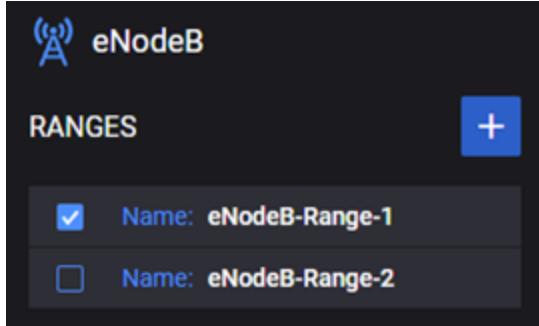
eNodeB RANGES panel	132
eNodeB RANGE panel	133
Cells settings	134
X2-C Interface Settings	135
X2-U Interface Settings	141
S1-C Interface Settings	142
S1-U Interface Settings	148

eNodeB RANGES panel

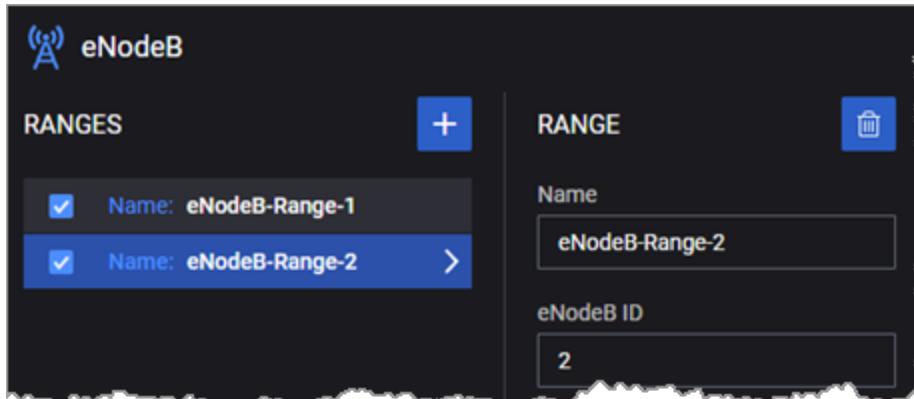
The eNodeB RANGES panel opens when you select the eNodeB node from the network topology window. You can perform the following tasks from this panel:

- 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, Cu Isolation 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 th 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 CU	Select the gNB-CU range to which this eNodeB is linked over the X2 interface.		
Use Secondary/Neighbor CU	<p>Select this option to enable inter-CU handovers. (Refer to the <i>Strategy</i> setting in Mobility settings 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 Associated CU)</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 Associated CU)
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 Associated CU)		

Setting	Description
	setting).
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.

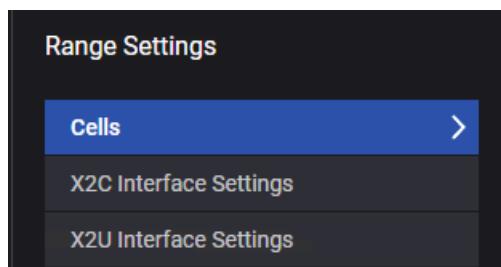
Range Settings:

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

Cells settings	134
X2-C Interface Settings	135
X2-U Interface Settings	141
S1-C Interface Settings	142
S1-U Interface Settings	148

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	Enter the value by which Cu Isolation will increment each Cell ID if the Cell Count

Setting	Description
Increment	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 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.

Setting	Description
	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 below](#)
- [VLAN Settings below](#)
- [IPsec Settings on the facing page](#)

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 Cu Isolation 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, Cu Isolation 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.
Inner IP Type	Select the IP type: IPv4 or IPv6.
<i>IP:</i>	
IP	The IP address of the S1C interface on the eNodeB range.
IP Address Increment	The IP address prefix assigned to this interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
IP Prefix Length	Set the IP address increment value.
Gateway Address	The IP address assigned as gateway address.
Role	<p><i>The role that this interface will play in the test:</i></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><i>The default value is Initiator (Site-to-Site).</i></p>
<i>Authentication settings:</i>	
Authentication Method	Select the authentication method to use in this configuration. The options are: <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 Cu Isolation Global settings. Refer to CA Certificates Settings 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</p>

Setting	Description
	<p>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>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 <i>-GCM</i> 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	<p>The hash algorithm to use for IPsec message exchanges.</p>
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

Setting	Description
	<p>Hash Algorithm 256.</p> <ul style="list-style-type: none"> • HMAC-SHA384: Hash-based Message Authentication Code, Secure Hash Algorithm 384. • HMAC-SHA512: Hash-based Message Authentication Code, Secure Hash Algorithm 512.
<i>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>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.

Setting	Description
	<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>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 (s)	<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>
IKE Retry Count	Enter the number of retries for IKE SA INIT or IKE AUTH request messages. 0 means that retry is disabled.
IKE Retry	This parameter determines how long the system waits before retransmitting an

Setting	Description
Timeout (s)	IKE message if a response is not received.

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 Cu Isolation 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.

Setting	Description
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 Cu Isolation to perform checksum computation for this range.
Gateway Address	This eNodeB node's gateway address towards X2AP interface of gNB-CU.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC settings:</i>	
MAC Address	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, Cu Isolation 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 below](#)
- [IPsec settings on the next page](#)

IP Settings

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

Setting	Description
IP	<p>Enter the IP address for the first eNodeB node in this range.</p> <p>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.</p>
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	<p>When <i>Outer VLAN</i> is enabled, Cu Isolation exposes the optional <i>Inner VLAN</i> setting.</p> <p>Enable this setting if you need inner VLAN IDs for your test, and then specify the inner VLAN ID.</p>

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.
Inner IP Type	Select the IP type: IPv4 or IPv6.
<i>IP:</i>	
IP Address	The IP address of the S1C interface on the eNodeB range.
IP Address Increment	The IP address prefix assigned to this interface. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
IP Prefix Length	Set the IP address increment value.
Gateway Address	The IP address assigned as gateway address.
Role	<p><i>The role that this interface will play in the test:</i></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><i>The default value is Initiator (Site-to-Site).</i></p>
<i>Authentication settings:</i>	
Authentication Method	Select the authentication method to use in this configuration. The options are: <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 Cu Isolation Global settings. Refer to CA Certificates Settings for instructions.
Certificate and Private Keys	To upload a zip file that contains the certificate file (extension .crt) and the private key (extension .key):

Setting	Description
	<p>1. In the <i>Certificates and Private Keys (.zip)</i> field, select the zip file.</p> <p>2. Click Upload.</p> <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>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 <i>-GCM</i> 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>

Setting	Description
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>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>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.

Setting	Description
	<ul style="list-style-type: none"> • 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>
IKE Phase 2	Specifies the Phase 2 Security Association (SA) lifetime, in

Setting	Description
(ESP) Lifetime	<p>seconds.</p> <p>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>
IKE Retry Count	Enter the number of retries for IKE SA INIT or IKE AUTH request messages. 0 means that retry is disabled.
IKE Retry Timeout (s)	This parameter determines how long the system waits before retransmitting an IKE message if a response is not received.

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.

Setting	Description
Include Sequence Number	Select this option if you want Cu Isolation to include sequence numbers in T-PDUs for this interface range.

Connectivity Settings

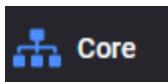
The connectivity settings include the IP address values plus the layer 2 values for the user plane traffic.

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 Cu Isolation to perform checksum computation for this range.
Gateway Address	This eNodeB node's gateway address towards S1 interface of the EPC.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC settings:</i>	
MAC Address	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

Setting	Description
	ID.
Inner VLAN	When Outer VLAN is enabled, Cu Isolation 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 12

Core configuration settings



In the 5G standalone (SA) topology, CoreSim simulates control plane traffic from the AMF over the N1 and N2 interfaces, and user plane traffic from the UPF over the N3 interface towards the NG-RAN.

The **Core** panel opens when you select the Core node from the network topology window.

You can perform the following tasks from this panel:

- Set the distribution mode for ranges and agents.
- Configure all settings for Core node.

If one or multiple agents are assigned to the Core node, the **Distribution Mode** parameter (see [Distribution Mode feature](#)) displays the available options in the drop-down:

- **All Ranges on All Agents** - This setting will configure all Core ranges on all agents.

Chapter contents:

Core Settings	152
N6/SGi interface settings	153
Core Ranges settings	154
AMF Ranges configuration settings	155
AMF node settings	156
AMF N2 interface settings	160
UPF Ranges configuration settings	160
UPF N3/S1-u/S5-u interface settings	161
MME Ranges configuration settings	162
MME node settings	163
MME S1 interface settings	165
SGW Ranges configuration settings	166
SGW S1-u interface settings	168
SEG Ranges configuration settings	168
SEG interface settings	172

N3IWF Ranges configuration settings	173
N3IWF interface settings	180

Core Settings

To configure the core settings, select **Core Settings** from the Core panel.

The following table describes the parameters required for core settings configuration.

Setting	Description
Home Network Private Key	The Home Network Private key that is used for subscriber privacy.
Interworking without N26 interface	When enabled, Core indicates that it supports interworking without N26 interface.
<i>Routing Indicators</i>	<p><i>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 provisioned in the USIM.</i></p> <p><i>You can add as many Routing Indicators as necessary to support your test objectives.</i></p>
	Select the Add Routing Indicator button to add a Routing Indicator.
	Select the Delete button to remove the routing indicator.
<i>PCRF Node Settings</i>	<i>You can enable or disable the PCRF Node Settings, as required by your test configuration.</i>
Origin Host Prefix	Set the origin host prefix. Default value: host .
Origin Realm	Set the origin realm. Default value: keysight.com .
<i>Rx Interface Settings</i>	<p><i>The Rx Interface Settings panel is available only when the PCRF Node Settings panel is enabled.</i></p> <p><i>The Rx interface settings are described below.</i></p>

Rx Interface Settings

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.

Connectivity Settings	Description
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Port	The port number to use for this interface communications. The default is port 3868, but you can choose a different port number.

N6/SGi interface settings

N6 is the interface between the UPF session anchor and the DN. It is the interconnection point at which user plane packet encapsulation and decapsulation is performed.

The following **Connectivity Settings** enable the necessary N6/SGi connectivity and service interaction.

Connectivity Settings	Description
Stack Type	Select the stack type from the drop-dpwn list. Available options: Single Stack or Dual Stack .
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	Maximum transmission unit.
MSS	Maximum segment size.
Secondary IP	<i>Select the IP address to open the secondary IP configuration panel for editing.</i> IMPORTANT <i>This panel is available only when the Stack Type is set to Dual Stack.</i>
IP Address	The IP address assigned as the gateway address for the external traffic source.

Connectivity Settings	Description
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

Core Ranges settings

When you select the Core Ranges pane ,Cu Isolation opens the Core Range panel, from which you can:

- Designate the node as a **Device Under Test**.
- Select the corresponding pane to configure the core range and connectivity settings:
 - [AMF Ranges](#)
 - [UPF Ranges](#)
 - [MME Ranges](#)
 - [SGW Ranges](#)

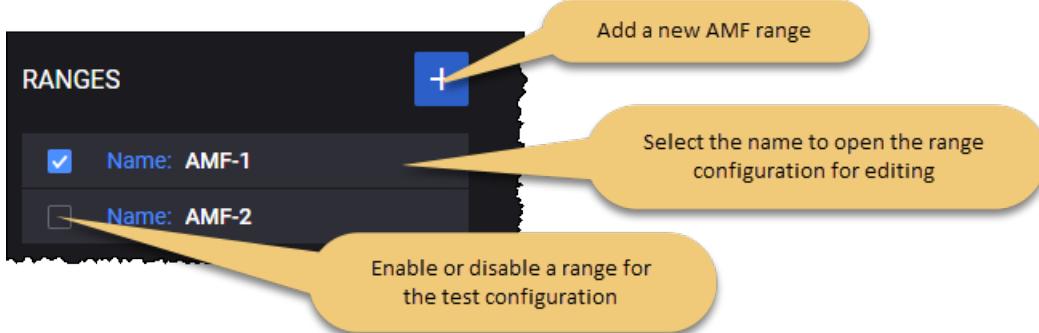
AMF Ranges configuration settings

To access and configure the AMF ranges settings, select **AMF Ranges** from the Core Ranges panel.

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

- Add a new AMF range to your test configuration.
- Open an AMF range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



You add and select AMF ranges from the Ranges panel. When you select the name of an AMF, the application opens the **Range** panel, from which you can:

- Delete the AMF range from the test configuration.
- Configure the node and connectivity settings for the AMF range.

AMF range controls and settings

Each AMF range is identified by a unique name. You can add and delete AMF ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each AMF range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	
Node Settings	Each AMF range requires the configuration of an associated set of Node Settings, which are described in AMF node settings .
N2 Interface Settings	Each AMF range requires the configuration of N2 interface settings, through which a AMF instance interacts with RAN in a 5G network. These settings are described in AMF N2 interface settings .

AMF node settings

Each AMF range includes a set of Node Settings.

Node Settings

Each AMF instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Instance ID	<p>Multiple AMF instances may be deployed in the 5G network.</p> <p>Each AMF instance is uniquely identified by an <i>Instance ID</i>. You can accept the value provided by Cu Isolation or overwrite it with your own value.</p>
Name	<p>The name uniquely identifies each AMF instance. You can accept the value provided by Cu Isolation or overwrite it with your own value.</p>
PLMN MCC	<p>The PLMN MCC for this AMF range.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this AMF range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Region ID	<p>An AMF Region consists of one or multiple AMF Sets.</p> <p>The AMF Region ID to use for this simulated AMF node. 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.</p>
Set ID	<p>An AMF Set consists of some AMFs that serve a given area and Network Slice. Multiple AMF Sets may be defined per AMF Region and Network Slice(s).</p> <p>The AMF Set ID to use for this simulated AMF node. The Set ID uniquely</p>

Setting	Description
	identifies the AMF Set within the AMF Region.
Pointer	The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.
Relative Capacity	Set the relative capacity value.
Ciphering Algorithm	Allows to select the supported 5G ciphering algorithm: <ul style="list-style-type: none"> • NEA0 - Null ciphering algorithm • NEA1 - 128-bit SNOW 3G based algorithm • NEA2 - 128-bit AES based algorithm • NEA3 - 128-bit ZUC based algorithm
Integrity Algorithm	Allows to select the supported 5G integrity protection algorithm: <ul style="list-style-type: none"> • NIA0 - Null Integrity Protection algorithm • NIA1 - 128-bit SNOW 3G based algorithm • NIA2 - 128-bit AES based algorithm • NIA3 - 128-bit ZUC based algorithm
Request N2 SM Information	Enable this option to request N2 SM Information again instead of using the existing one.
Prefer AMF Change	Enable this option to change the AMF for an N2 handover even when the target RAN(T-RAN) is connected to the serving AMF.
Skip MT SMS	If enabled, it will skip the initiation of the MT SMS procedure when the MO SMS procedure ends.

T3512: Select the check box to open T3512 Settings and configure the T3512 timer.

NOTE

If disabled, a value of 50 minutes (Value 5 X Unit 10 minutes) is sent for T3512.

Value	Set the value for this parameter. The accepted values are between 0-31.
Unit	Select the unit size for this parameter from the drop-down list.
NSSAI	<i>These settings are described below.</i>
TAI	<i>These settings are described below.</i>
Public Warning System	<i>These settings are described below.</i>
Emergency Settings	<i>These settings are described below.</i>

NSSAI

The following table describes the configuration settings that are required for NSSAI.

Setting	Description												
<i>NSSAI:</i>													
	Select the Add NSSAI button to add a new NSSAI to your test configuration.												
<i>NSSAI settings:</i>													
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.												
SST	<p>The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:</p> <table border="1"> <thead> <tr> <th>SST</th> <th>Value</th> <th>Suitable for handling:</th> </tr> </thead> <tbody> <tr> <td>eMBB</td> <td>1</td> <td>5G enhanced Mobile Broadband</td> </tr> <tr> <td>URLCC</td> <td>2</td> <td>ultra-reliable low-latency communications</td> </tr> <tr> <td>MIoT</td> <td>3</td> <td>massive IoT</td> </tr> </tbody> </table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
SST	Value	Suitable for handling:											
eMBB	1	5G enhanced Mobile Broadband											
URLCC	2	ultra-reliable low-latency communications											
MIoT	3	massive IoT											
SD	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 NSSAI.												

TAI

The following table describes the configuration settings that are required for TAI.

Setting	Description
<i>TAI:</i>	
	Select the Add TAI button to add a new TAI (Tracking Area Identity) to your test configuration.
<i>TAI settings:</i>	
	Select the Delete TAI button to delete this TAI from your test configuration.
<i>PLMN ID: Set the values for the PLMN identifier.</i>	
PLMN MCC	The PLMN Mobile Country Code (MCC) used in the construction of the TAI.
PLMN MNC	The PLMN Mobile Network Code (MNC) used in the construction of the TAI.

Setting	Description
<i>TAC:</i>	
	Select the Add TAC button to add a new TAC (Tracking Area Code) to your test configuration.
<i>Settings:</i>	
	Select the Delete TAC button to delete this TAC from your test configuration.
TAC	The Tracking Area Code (TAC) used in the construction of the TAI.

Public Warning System

The following table describes the configuration settings that are required for public warning system.

Setting	Description
Message ID	Set the public warning system message ID.
Repetition Period	Set the public warning system message repetition period.
Number of Broadcasts Requested	Set the public warning system message number of requested broadcasts.
Time to Wait Before Triggering PWS after NG Setup (s)	Set the number of seconds to wait before triggering PWS after NG setup.
PWS Cancel Timer (s)	Duration in seconds after which PWS cancel warning is sent. 0 indicates no cancellation.

Emergency Settings

The following table describes the emergency settings configuration.

Setting	Description
Authentication Behaviour	<p>The authentication procedure behaviour during an Emergency Registration.</p> <p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> • Normal Authentication (default value) • Allow Authentication Failure • Skip Authentication
Emergency Services Support Value	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> • Not Supported (default value) • In NR connected to 5GC only • In EUTRA connected to 5GC only

Setting	Description
	<ul style="list-style-type: none"> • In NR connected to 5GC and EUTRA connected to 5GC
Emergency Services Fallback Support Value	Select an option from the drop-down list: <ul style="list-style-type: none"> • Not Supported (default value) • In NR connected to 5GC only • In EUTRA connected to 5GC only • In NR connected to 5GC and EUTRA connected to 5GC

AMF N2 interface settings

N2 is the service-based interface through which a AMF instance interacts with RAN in a 5G network.

The following **Connectivity Settings** enable the necessary N2 connectivity and service interaction.

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix that has been assigned to this node.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

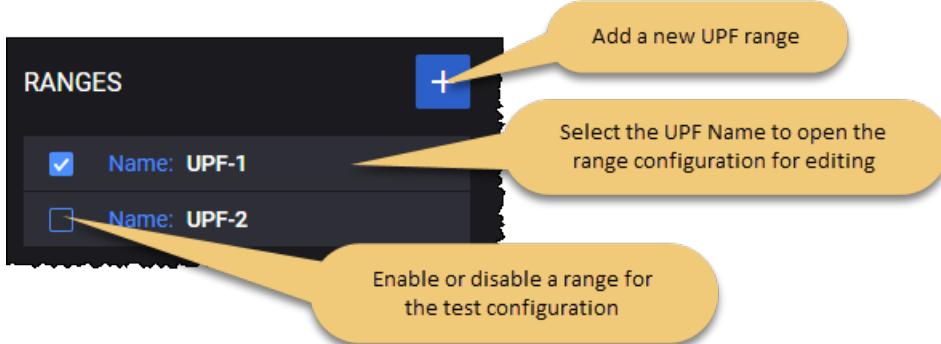
UPF Ranges configuration settings

To access and configure the UPF ranges settings, select **UPF Ranges** from the Core Ranges panel.

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

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

For example ...



You add and select UPF ranges from the Ranges panel. When you select an UPF range *Name*, the application opens the **Range** panel, from which you can:

- Delete the UPF range from the test configuration.
- Modify the UPF range name.
- Configure interface settings for the UPF range.

The following table describes the **Range Settings** that you configure for each UPF range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Name	The name of the UPF range. You can accept the name provided by the Cu Isolation, or you can replace it with a name of your own choosing.
Range Count	The number of UPFs in the UPF range.
<i>Range Settings:</i>	
N3/S1-u/S5-u Interface Settings	N3 is the interface between the RAN and the UPF. These interface settings are described in UPF N3/S1-u/S5-u interface settings .

UPF N3/S1-u/S5-u interface settings

The following configuration settings are required by each UPF N3 range.

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	Maximum transmission unit.
MSS	Maximum segment size.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

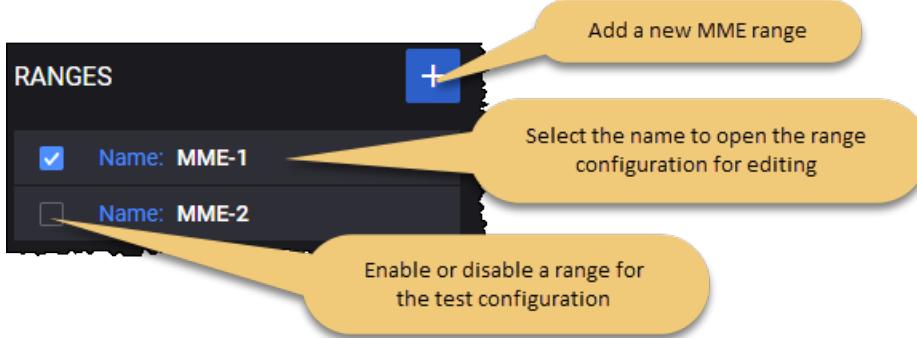
MME Ranges configuration settings

To access and configure the MME ranges settings, select **MME Ranges** from the Core Ranges panel.

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

- Add a new MME range to your test configuration.
- Open an MME range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



You add and select MME ranges from the MME Ranges panel. When you select the name of an MME , the application opens the **Range** panel, from which you can:

- Delete the MME range from the test configuration.
- Configure the node and connectivity settings for the MME range.

MME range controls and settings

Each MME range is identified by a unique name. You can add and delete MME ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each MME range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	
Node Settings	Each MME range requires the configuration of an associated set of Node Settings, which are described in MME node settings .
S1 Interface Settings	These settings are described in MME S1 interface settings .

MME node settings

Each MME range includes a set of Node Settings.

Node Settings

Each MME instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Name	The name uniquely identifies each MME instance. You can accept the value provided by Cu Isolation or overwrite it with your own value.

Setting	Description
Group ID	Set the MME group ID value.
Code	Set the MME code value.
PLMN MCC	<p>The PLMN MCC for this MME range.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this MME range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Ciphering Algorithm	<p>Allows to select the supported 5G ciphering algorithm:</p> <ul style="list-style-type: none"> • EEA0 - Null ciphering algorithm • EEA1 - 128-bit SNOW 3G based algorithm • EEA2 - 128-bit AES based algorithm • EEA3 - 128-bit ZUC based algorithm
Integrity Algorithm	<p>Allows to select the supported 5G integrity protection algorithm:</p> <ul style="list-style-type: none"> • EIA0 - Null Integrity Protection algorithm • EIA1 - 128-bit SNOW 3G based algorithm • EIA2 - 128-bit AES based algorithm • EIA3 - 128-bit ZUC based algorithm
Relative Capacity	Set the relative capacity value.
Public Warning System	<i>Select the check box to enable this option.</i>
Message ID	<p>Set the public warning system message ID. Values should be in range 0-65535.</p> <p>Default value: 4352.</p>

Setting	Description
Repetition Period	Set the public warning system message repetition period. Values should be in range 1-131071. Default value: 1 .
Number of Broadcasts Requested	Set the public warning system message number of requested broadcasts. Values should be in range 0-65535. Default value: 1 .
Time to Wait Before Triggering PWS after NG Setup (s)	Set the number of seconds to wait before triggering PWS after S1 setup. Values should be in range 0-86400. Default value: 1 .
PWS Kill Timer (s)	Duration in seconds after which PWS Kill Request is sent. Values should be in range 0-86400. Default value: 0 .

MME S1 interface settings

The following **Connectivity Settings** enable the necessary S1 connectivity and service interaction.

S1 Interface Settings	Description
Local STCP Port	Set the local STCP port number.
<i>Connectivity Settings</i>	
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.

S1 Interface Settings	Description
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route from your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

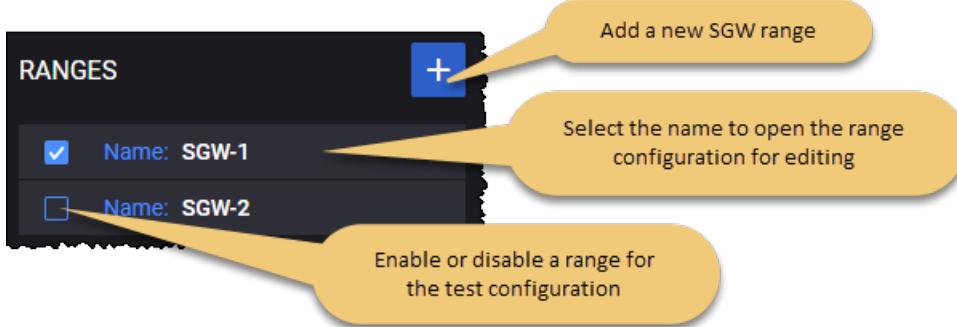
SGW Ranges configuration settings

To access and configure the SGW ranges settings, select **SGW Ranges** from the Core Ranges panel.

You can perform the following tasks from the **SGW Ranges** panel:

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

For example ...



You add and select SGW ranges from the Ranges panel. When you select the name of a SGW, the application opens the **Range** panel, from which you can:

- Delete the SGW range from the test configuration.
- Modify the SGW range name.
- Configure the range and connectivity settings for the SGW range.

SGW range controls and settings

Each SGW range is identified by a unique name. You can add and delete SGW ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each SGW range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Name	The name uniquely identifies each SGW instance. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Range Count	The number of SGWs in the SGW range.
<i>Range Settings:</i>	
UDP Rx Buffer (bytes)	Size of receive buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 #The default Linux buffer size • maximum: 134217728 #128MB • default: 12582912 #12MB
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 # The default Linux buffer size • maximum: 134217728 #128MB • default: 2097152 #2MB
S1-u	These settings are described in SGW S1-u interface settings .

Setting	Description
Interface Settings	

SGW S1-u interface settings

The following **Connectivity Settings** enable the necessary S1-u connectivity and service interaction.

S1-u Interface Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

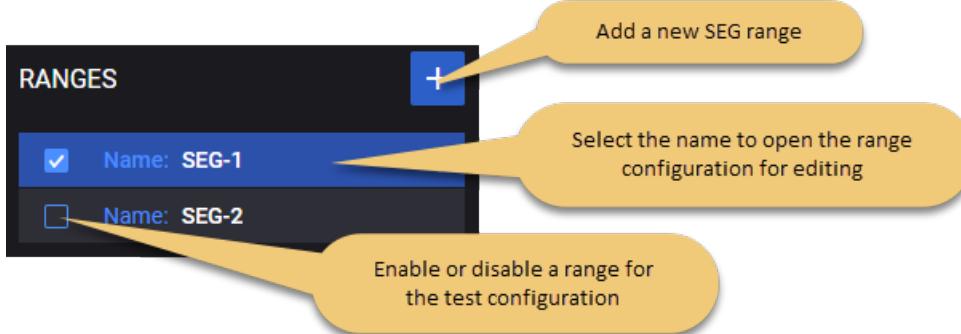
SEG Ranges configuration settings

To access and configure the SEG ranges settings, select **SEG Ranges** from the CoreSim panel.

You can perform the following tasks from the **SEG Ranges** panel:

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

For example ...



You add and select SEG ranges from the SEG Ranges panel. When you select the name of a SEG , the application opens the **Range** panel, from which you can:

- Delete the SEG range from the test configuration.
- Designate the range as a **Device Under Test**.
- Modify the SEG range name.
- Configure the range and connectivity settings for the SEG range.

SEG range controls and settings

Each SEG range is identified by a unique name. You can add and delete SEG ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each SEG range.

Setting	Description
<i>Range:</i>	
Device Under Test	Enable this option if your SEG is a DUT in this test configuration. When this option is not enabled, the Cu Isolation will simulate the SEG functionality (if it is selected in the Topology window).
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	
<i>Node Settings</i>	
Name	The name uniquely identifies each SGW instance. You can accept the value provided by Cu Isolation or overwrite it with your own value.

Setting	Description
Role	By default, the role is set to Responder (Remote Access) and cannot be changed.
UDP Rx Buffer (bytes)	Size of receive buffers for UDP sockets: <ul style="list-style-type: none"> minimum: 212992 maximum: 134217728 default: 12582912
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> minimum: 212992 maximum: 134217728 default: 2097152
Interface Settings	<i>These settings are described in SEG interface settings.</i>
<i>Remote Access IP Pool</i>	
IP Address	Set the start IP address.
IP Increment	Set the IP address increment value.
IPs count	Set the IP count value.
IP Prefix Length	Set the IP prefix length value.
Local Protected Subnet	<i>Selects which node(s) are protected by SEG: AMF and/or UPF . AMF and UPF could be protected by the same SEG when running with Linux stack.</i>
N2 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific AMF range from the list.
N3 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific UPF range from the list.
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to Certificates and cannot be changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	It allows you to upload an archive that contains the certificates and keys for the SEG range, using the Upload button. To remove the archive , select the Clear button. The <code>.key</code> and <code>.crt</code> files need to have the same name before extensions.
Use Same Certificates and	By default, this option is disabled. Select the toggle button to enable it.

Setting	Description
Private Key For All Tunnels	
<i>IKE Phase 1</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	<p>Select an option from the drop-down list.</p> <p>Default value: prime256v1(19). Available options: prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32).</p>
PRF Algorithm	<p>Select an option from the drop-down list.</p> <p>Default value: HMAC-SHA256. Available options: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512.</p>
<i>IKE Phase 2</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i>

Setting	Description
	<p>is NONE.</p> <ul style="list-style-type: none"> If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list.</p> <p>Default value: ID_DER ASN1 DN. Available options: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER ASN1 DN, ID_KEY_ID.</p>
Local Identification Value	<p>Set the value for this parameter.</p> <p>This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR.</p>
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
DPD Interval (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>

SEG interface settings

The following **Connectivity Settings** enable connectivity and service interaction.

SEG Interface Settings	Description
Source Port	Set the source port number.
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.

SEG Interface Settings	Description
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MAC	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

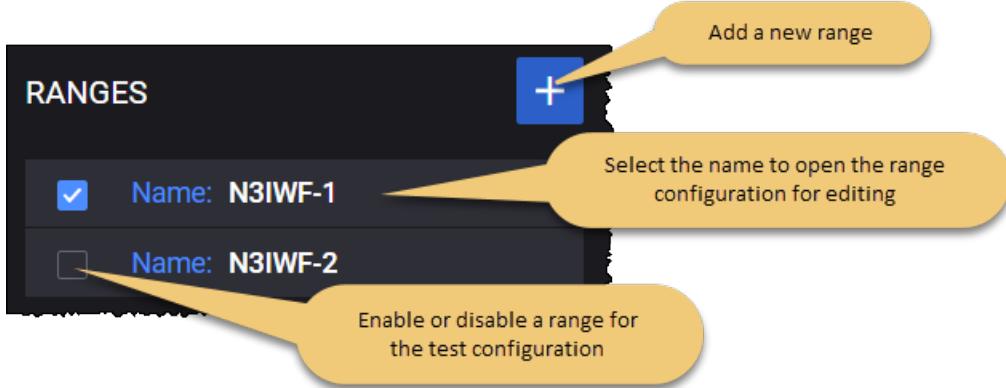
N3IWF Ranges configuration settings

To access and configure the N3IWF ranges settings, select **N3IWF Ranges** from the CoreSim panel.

You can perform the following tasks from the **N3IWF Ranges** panel:

- Add a new N3IWF range to your test configuration.
- Open a N3IWF range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



You add and select N3IWF ranges from the N3IWF Ranges panel. When you select the name of a N3IWF, Cu Isolation opens the **Range** panel, from which you can:

- Delete the N3IWF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Modify the N3IWF range name.
- Configure the range and connectivity settings for the N3IWF range.

N3IWF range controls and settings

Each N3IWF range is identified by a unique name. You can add and delete N3IWF ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each N3IWF range.

Setting	Description
<i>Range:</i>	
Device Under Test	Enable this option if your N3IWF is a DUT in this test configuration. When this option is not enabled, the Cu Isolation will simulate the N3IWF functionality (if it is selected in the Topology window).
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	
<i>Node Settings</i>	
Name	The name uniquely identifies each N3IWF instance. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Role	By default, the role is set to Responder (Remote Access) and cannot be changed.
PLMN MCC	The PLMN MCC for this N3IWF range. About PLMN MCC ...

Setting	Description
	<p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this N3IWF range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Tracking Area Code	Provide the Tracking Area Code (TAC) value
N3IWF ID	Set the value for this field.
N3IWF ID Increment	Set the increment value for this field.
SCTP Tx Buffer (bytes)	Set the size of SCTP Tx Buffer.
SCTP Rx Buffer (bytes)	Set the size of SCTP Rx Buffer.
UDP Rx Buffer (bytes)	<p>Size of receive buffers for UDP sockets:</p> <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 12582912
UDP Tx Buffer (bytes)	<p>Size of transmit buffers for UDP sockets:</p> <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 2097152
<i>Traffic Profiles</i>	<i>These settings are described in Traffic Profiles settings.</i>
<i>NSSAI</i>	<i>These settings are described in NSSAI settings.</i>
<i>NWu Interface</i>	<i>These settings are described in NWu interface settings.</i>

Setting	Description
Settings	
N2 Interface Settings	These settings are described in N2 interface settings .
N3 Interface Settings	These settings are described in N3 interface settings .
<i>Authentication</i>	
Configure Certificates	By default, this option is disabled. When enabled, the following fields become available: <i>Certificates(.zip)</i> and <i>Use Same Certificate For All Instances</i> .
CA Certificate	Select the CA Certificate from the drop-down list. <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> NOTE To be able to populate and select from the drop-down, you first need to upload certificates. </div>
Certificates (.zip)	It allows you to upload an archive that contains the certificates for the N3IWF range, using the Upload button. To remove the archive , select the Clear button.
Use Same Certificates For All Instances	By default, this option is disabled. Select the toggle button to enable it.
<i>IKE Phase 1</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16 .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: NONE . Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 . Restrictions: <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	Select an option from the drop-down list. Available options are: modp768(1), modp1024(2), modp1536(5), modp2048(14), modp3072(15), modp4096(16), modp6144(17), modp8192(18), prime256v1(19) ,

Setting	Description
	<p>secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32). Default value: prime256v1(19).</p>
PRF Algorithm	<p>Select an option from the drop-down list. Default value: HMAC-SHA256. Available options: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512.</p>
IKE Phase 2	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list. Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256. Restrictions:</p> <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
Identification	
Local Identification Type	<p>Select an option from the drop-down list. Default value: ID_DER_ASN1_DN. Available options: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER_ASN1_DN, ID_KEY_ID.</p>
Local Identification Value	<p>Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR.</p>
Timers	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter. Default value: 0 (disabled).</p>

Setting	Description
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: 0 (disabled).

Traffic Profiles

The following table describes the configuration settings that are required for Control Plane.

NOTE Only one Control Plane Profile is accepted.

Setting	Description
TCP Port	The TCP port for N3IWF: <ul style="list-style-type: none"> default value: 20000. minimum value: 1024. maximum value: 65535.
IP Type	Select the IP type from the drop-down list: IPv4 (default) or IPv6 .
Local Protected Subnet IP Address	The IP address for N3IWF TCP server. Default value: 150.0.2.1 .
Local Protected Subnet IP Prefix Length	The only accepted options are 32 for IPv4 and 128 for IPv6.
Remote Inner IP Address	Per UE IP Address used for TCP Control Plane connection. Address increment is 1. Default value: 150.0.100.1 .

The following table describes the configuration settings that are required for User Plane.

NOTE A maximum of 15 User Plane Profile can be configured.

Setting	Description
	Select the Add User Plane button to add a new profile to your test configuration.
	Select the Delete User Plane button to delete this profile from your test configuration.
DNN	Select the DNN value for the drop-down list.
IP Type	Select the IP type from the drop-down list: IPv4 (default) or IPv6 .

Setting	Description
Local Protected Subnet IP Address	The IP address for N3IWF GRE endpoint. Default value: 150.1.2.1 .
Local Protected Subnet IP Prefix Length	The only accepted options are 32 for IPv4 and 128 for IPv6.
Remote Inner IP Address	Per PDU Session IP Address used for GRE User Plane connection. Address increment is 1. Default value: 150.1.100.1 .

NSSAI

The following table describes the configuration settings that are required for NSSAI.

Setting	Description												
<i>NSSAI:</i>													
	Select the Add NSSAI button to add a new NSSAI to your test configuration.												
<i>NSSAI settings:</i>													
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.												
SST	<p>The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:</p> <table border="1"> <thead> <tr> <th>SST</th> <th>Value</th> <th>Suitable for handling:</th> </tr> </thead> <tbody> <tr> <td>eMBB</td> <td>1</td> <td>5G enhanced Mobile Broadband</td> </tr> <tr> <td>URLCC</td> <td>2</td> <td>ultra-reliable low-latency communications</td> </tr> <tr> <td>MIoT</td> <td>3</td> <td>massive IoT</td> </tr> </tbody> </table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
SST	Value	Suitable for handling:											
eMBB	1	5G enhanced Mobile Broadband											
URLCC	2	ultra-reliable low-latency communications											
MIoT	3	massive IoT											
SD	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 NSSAI.												

N3IWF interface settings

NWu interface settings

The following settings enable connectivity and service interaction.

Interface Settings	Description
Source Port	Set the source port number.
Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

N2 interface settings

The following settings enable connectivity and service interaction.

Interface Settings	Description
Peer AMF	The IP address of the AMF node connected 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 36412, but you can change it.
Connection Timeout (ms)	Set the connection timeout value.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
<i>MAC</i>	Select the MAC address to open the MAC configuration panel for editing.
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
<i>Outer VLAN</i>	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.

Connectivity Settings	Description
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

N3 interface settings

The following **Connectivity Settings** enable connectivity and service interaction.

SEG Interface Settings	Description
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MAC	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN is selected.</i></p>

SEG Interface Settings	Description
	<i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.

CHAPTER 13

IMS configuration settings

The IP Multimedia Subsystem (IMS) is a standards-based architectural framework for delivering multimedia communications services such as voice, video and text messaging over IP networks. IMS enables secure and reliable multimedia communications between diverse devices across diverse networks.

In Cu Isolation, IMS has two important components:

- Call Session Control Function (CSCF) – the core of the IMS architecture, responsible for controlling sessions between endpoints (referred to as terminals in the IMS specifications) and applications.
- Media Function

The configuration settings for these two components are described in the topics listed below.

Topics:

CSCF Range panel	184
Media Function Range panel	186

CSCF Range panel

When you select the CSCF's IP address from the **CSCF Ranges** panel, Cu Isolation opens the **Range** panel, from which you can select **CSCF Settings** to configure the node and connectivity settings for the CSCF range.

CSCF range controls and settings

The following table describes the available **Range** configuration options for the CSCF range.

Setting	Description
<i>P-CSCF Node Settings</i>	
Domain	Set the domain name.
Port	Set the port number. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Force IPsec Null Encryption	If enabled, it forces IPsec null encryption, therefore not encrypting the ESP traffic.
<i>SIP Settings</i>	

Setting	Description
Enable Retransmission	If enabled, it will allow the independent message exchanges. A SIP transaction consists of a single request and any responses to that request. The transaction layer handles application-layer retransmissions, matching of responses to requests, and application-layer timeouts.
Enable Retransmission for TCP Transport	<p>IMPORTANT This parameter can be enabled only if Enable Retransmission is on.</p> <p>If enabled, it will allow the message exchange for TCP transport.</p>
Timer T1 Value (ms)	T1 is an estimate of the RTT between the client and server transactions. A larger value is possible (recommended on high latency access links) if you know the RTT is larger. Default value is 500 ms.
Timer T2 Value (ms)	T2 is the maximum retransmit interval for non-INVITE requests and INVITE responses. If a provisional response is received, retransmissions continue for unreliable transports, but at an interval of T2. The default value is 4000 ms.
Timer T4 Value (ms)	T4 represents the maximum duration a message will remain in the network. The default value is 5000 ms.
Timer C Value (ms)	Time C is the proxy INVITE transaction timeout. The value must be larger than 3 minutes.
Timer D Value (ms)	Timer D represents the wait time for response retransmit.
<i>Authentication Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: keysight.com .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: Digest , AKAv2 or AKAv1 .
Algorithm	Select the algorithm from the drop-down list. Available options: MD5 , MD5-Sess , SHA256 or SHA256-Sess .
Quality of Protection	Select an option from the drop-down list: auth or auth-init .
Connectivity Settings	
IP Address	Set the IP address.

Media Function Range panel

When you select the Media Function's IP address from the **Media Function Ranges** panel, Cu Isolation opens the **Range** panel, from which you can configure the connectivity settings for the Media Function range.

Media Function range controls and settings

The following **Connectivity Settings** enable the necessary connectivity and service interaction.

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.

CHAPTER 14

DN configuration settings



Data Networks (DN) represents one of the entities in the 5G core network architecture. DN interfaces enable access to the public Internet, operator services, and other external data networks.

The configuration settings are described in the topics listed below.

Topics:

DN Ranges panel	187
DN Range panel	188
DN N6 interface settings	189
DN routes settings	190
DN User Plane	190
DN Attacks	192
DN Stateless UDP Traffic	192
Data Traffic	193
DN Voice Traffic	197
DN Video OTT Traffic	209
DN DNS Server Traffic	214
DN Predefined Applications Traffic	216
DN Capture Replay	216
DN Synthetic	218
DN UDG	220
DN Throttling settings	222

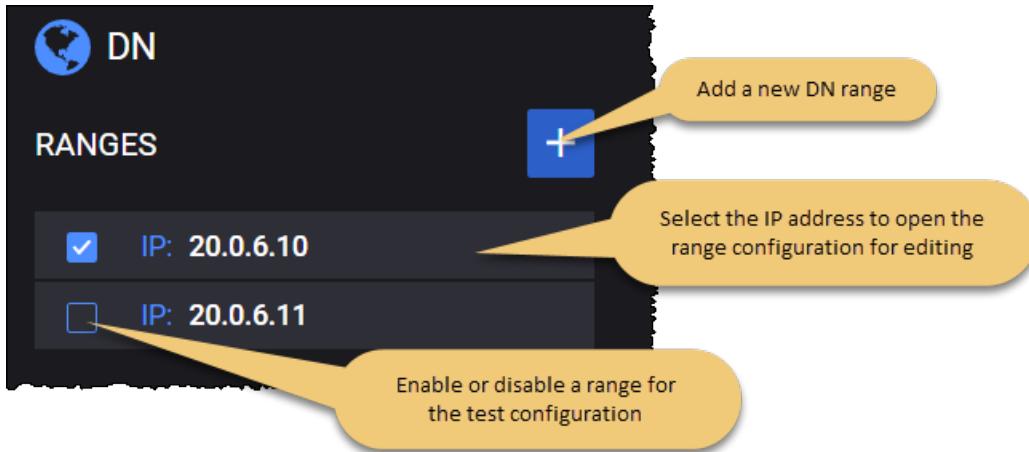
DN Ranges panel

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

- Add a new DN range to your test configuration.
- Open a DN range configuration (for editing or viewing).

- Enable or disable a range for the test configuration.

For example ...



DN Range panel

You add and select DN ranges from the DN Ranges panel. When you select a DN's IP address from the **UDR Ranges** panel, Cu Isolation opens the **Range** panel, from which you can:

- Select the **Delete Range** button to delete the DN range from the test configuration.
- Select **Range Settings** to configure the node and connectivity settings for the DN range.
- Select **Routes Settings** to configure the route to an UE or custom range.
- Select **User Plane** to configure the traffic generators.

DN range controls and settings

Each DN range is identified by a unique IP address. You can add and delete DN ranges as necessary to support your test objectives. For example, a test may require a range of UEs to concurrently access multiple data networks (for example, local and central DNS) using a single or multiple PDN sessions. In this case, you would create one DN range for each of those data networks.

The following table describes the available **Range** configuration options for each DN range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Range Count	The number of DNs in the DN range.
<i>Range Settings:</i>	
N6 Interface Settings	Each DN range requires the configuration of N6 interface settings, through which a DN instance enables connectivity and interaction with other functions in the 5G network. These settings are described in DN N6 interface settings .

Setting	Description
Routes Settings	These settings are described in DN routes settings .
User Plane	These settings are described in DN User Plane .
Throttling Settings	These settings are described in Throttling settings .

DN N6 interface settings

N6 is the interface between the Data Network (DN) and the UPF.

The following table describes the **Connectivity Settings** that you configure for each DN range.

Connectivity Settings	Description
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

Connectivity Settings	Description
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</p>
VLAN ID	VLAN identifier..
VLAN TPID	VLAN tag protocol ID.

DN routes settings

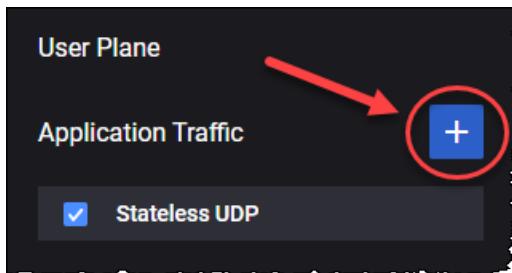
IMPORTANT This configuration set appears only if an agent is assigned to the DN node (wherever possible).

The following table describes the **Route Settings** that you need to configure in order to create the route to an UE or custom range.

Settings	Description
<i>Routes Config:</i>	
	Select this button to add a new route to a specific UE range or a custom one.
<i>UE Routes Config:</i>	
	Select this button to remove the route.
Route Type	Select the route type from the drop-down list. Available options: UE or Custom .
Destination Subnet Address	<p>Set the destination subnet address.</p> <p>This parameter is available only when the route type is set to Custom.</p>
IP Prefix Length	<p>The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.</p> <p>This parameter is available only when the route type is set to Custom.</p>
Gateway Address	<p>The IP address assigned as gateway address.</p> <p>This parameter is available only when the route type is set to Custom.</p>

DN User Plane

Cu Isolation provides multiple traffic application that can be added by selecting the **Add Objective** button.

**NOTE**

Based on your test requirements, the configuration of the User Plane Objectives may involve settings for the traffic generators on the UE and also on the DN. For the UE User Plane settings, refer to [UE User Plane](#).

Parameter	Description
	Select this button to add a new application traffic objective. The objective can be: <ul style="list-style-type: none"> • Attacks • Capture Replay • Data • DNS Server • Predefined Applications • Stateless UDP • Synthetic • UDG • Video OTT • Voice
	Select this button to remove the application traffic objective from your test configuration.
Stateless UDP	For the settings required to configure the Stateless UDP traffic objective, refer to DN Stateless UDP Traffic .
Data	For the settings required to configure the Data traffic objective, refer to DN Data Traffic .
Voice	For the settings required to configure the Voice traffic objective, refer to DN Voice Traffic .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to DN Video OTT Traffic .
DNS Server	For the settings required to configure the DNS Server objective, refer to DN DNS Client Traffic .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to DN Predefined Applications Traffic .

Parameter	Description
Synthetic	For the settings required to configure the Synthetic objective, refer to DN Synthetic .
UDG	For the settings required to configure the UDG objective, refer to DN UDG .
Capture Replay	For the settings required to configure the Capture Replay objective, refer to DN Capture UDP .
Attacks	For the settings required to configure the Capture Replay objective, refer to DN Attacks .

DN Attacks

The **Attacks** objective simulates multiple type of attacks (more than 7000 of profile attacks available).

The following table describes the Attacks parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Attacks .
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Attacks profile	Select the attack profile defined in the UE Ranges > User Plane Objectives > Attacks .

DN Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Flow Type	This field is set to dowlink and can not be modified since on the DN you can only configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.

Parameter	Description
Limit Maximum Packet Rate per Client	If enabled, it will limit the Maximum Packet Rate per DN.
Payload Size	The size of the packet payload, in bytes.
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.
Destination UE Range	Select the destination UE range from the drop-down list.
Start After First Uplink Packet	If this option is enabled, the downlink traffic will only start after the uplink traffic is received.

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 .
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
<i>TCP Settings</i>	<i>Select the panel to open the TCP settings.</i>
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	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.

Parameter	Description
Transmit buffer size (bytes)	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).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	Select the toggle button to enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
<i>TLS Settings</i>	See TLS Settings table for more details.
<i>Application Servers</i>	<p><i>Each Application Traffic entry requires an application server definition, and can support multiple such definitions.</i></p> <ul style="list-style-type: none"> <i>To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.</i>

Parameter	Description
	<ul style="list-style-type: none"> To add another application server, click the Add Server button. Cu Isolation will open the Server panel where you will select the server type and configure the server settings. <p>Refer to Server (below) for a description of the configuration settings required by the application server.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

TLS Settings

Parameter	Description
TLSv1.2	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.2 is selected.</p>
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> Disable Session ticket Session ID <p>IMPORTANT Session reuse method is available only if TLSv1.2 is selected.</p>
TLSv1.3	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Middlebox compatibility	<p>Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.
Certificate File	Select Upload to add your certificate file or Clear to remove it.

Parameter	Description
Key File	Select Upload to add your key file or Clear to remove it.
Key File Password	Enter your key file password.
DH file	Select Upload to add your DH file or Clear to remove it.

Server

You can add and delete application servers as needed to meet your test objectives. The **Server** parameters are described in the following table.

Parameter	Description
	Click the Delete Server button to remove the application server from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: TCP , TLS , QUIC or UDP .
Type	Select the L4/L7 protocol type from the list of pre-defined application servers. The available types include: <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get Responder, HTTP Put Responder, HTTP Post Responder, HTTP Server and FTP Responder. For TLS transport protocol: HTTPS Get Responder, HTTPS Put Responder, HTTPS Post Responder and HTTPS Server. For QUIC transport protocol: HTTP3 Server. For UDP transport protocol: UDP Bidirectional Responder.
Port	The port used by the application server.
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 FTP server.
Rx Packet Count	Add a value to the Rx packet count. This option appears only if Transport Protocol available for Data is set to UDP .
Tx Packet Count	Add a value to the Tx packet count. This option appears only if Transport Protocol available for Data is set to UDP .
Custom Parameters	See Custom Parameters/Headers for more details.

Custom Parameters/Headers

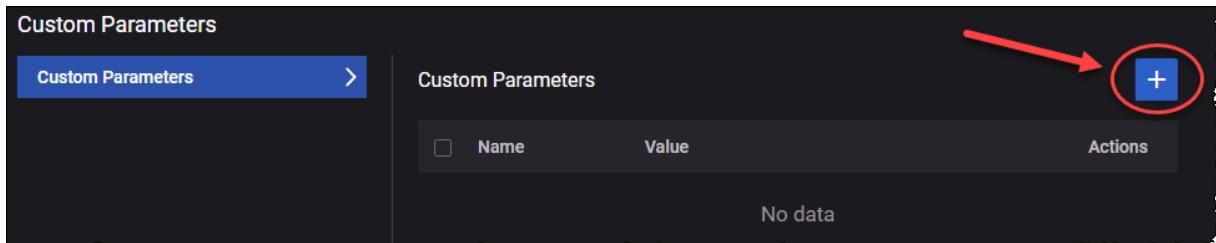
You can add custom parameters as follows:

1. Select the **Open Custom Parameters** button.



The Custom Parameters/Custom Headers panel opens.

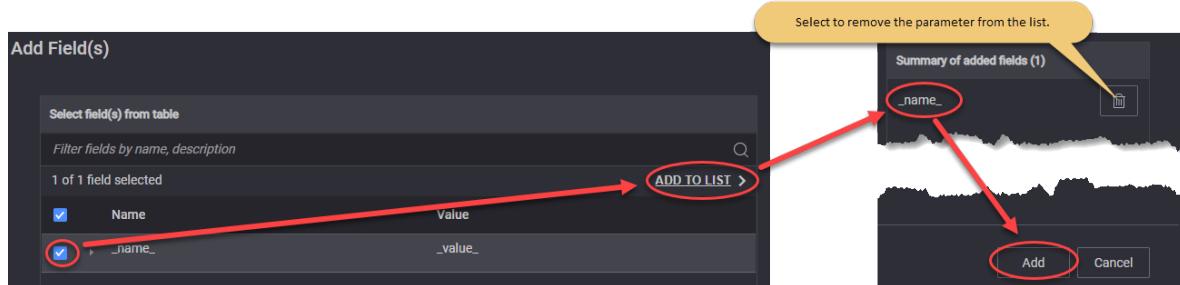
2. Select the **Add** button.



The Add Field(s) opens.

3. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



4. Once added in the Custom tables, you can edit the value, or press the Menu icon (⋮) to Edit name or Delete the new parameter/header. You can also reorder the items in these tables by dragging them up or down.

DN 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 .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be

Parameter	Description
	generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Call Type	Select the type of call from the drop-down list.
Dial Plan:	<i>For the settings required to configure the dial plan, refer to Dial Plan.</i>
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by Cu Isolation 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 • UDP - User Datagram Protocol
Domain	Provide the domain name.
Advanced SIP Settings	<i>For more details about these settings, refer to Advanced SIP Settings.</i>
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by Cu Isolation or overwrite it with your own value.
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 the check box in order to enable this option.
RTP Session Duration (ms)	Set the value for the session duration.
Audio settings:	<i>For the configuration of audio settings, refer to Audio Settings.</i>
Video Settings:	<i>For the configuration of video settings, refer to Video Settings.</i>
MSRP Settings:	<i>For the configuration of MSRP settings, refer to MSRP Settings.</i>

Parameter	Description
MCTTP Settings	For the configuration of MCTTP settings, refer to MCPTT Settings .
<i>Advanced Media Settings:</i>	
Custom SDP	Select this panel to open the custom SDP settings.
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4 • NB Codecs IPv6 • AMR-WB IPv6 • Multimedia IPv4
QoE Settings	Select this panel to open the audio QoE settings.
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

Dial Plan

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

Parameter	Description
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.

Audio Settings

The parameters required for audio settings are presented in the table below.

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for audio from the drop-down list.
<i>Jitter Buffer Settings:</i>	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).

Parameter	Description
<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 - 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-WB - 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 - 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 <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

Parameter	Description
	implementations efficient. All fields of an AMR payload (payload header, table of contents and speech) are individually octet aligned.
Bitrate	Indicates the mode(bitrate) of the AMR codec. For AMR there are 8 available modes. All these modes can be changed dynamically without negotiation, reflecting the main characteristics of this codec – adaptive rate. For AMR WB there are 9 modes available.

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	The following options are available: <ul style="list-style-type: none"> Full header - 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 Settings

The parameters required for audio settings are presented in the table below.

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Voice	Select the QoS Flows ID(s) from the drop-down list.

Parameter	Description
Video Codecs	<i>This section is available only when Enable video is selected</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	Select the audio codec from the drop-down list. The available options are: H264 or H265 .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

MSRP Settings

The parameters required for MSRP settings are presented in the table below.

Parameter	Description
Enable MSRP	Select to enable this option.
QoS Flow ID for MSRP	Select the QoS Flows ID(s) from the drop-down list.
MSRP Port	Provide the MSRP port.
MSRP Local domain	Provide the MSRP local domain.

MCPTT Settings

The parameters required for Mission Critical Push to Talk (MCPTT) settings are presented in the table below.

Parameter	Description
Enable MCPTT	Select to enable this option.
QoS Flow ID for MCPTT	Select the QoS Flows ID(s) from the drop-down list.
MCPTT Message Format	The MCPTT message format defined according to TS 24.380 standard.
MCPTT Group	A defined set of MCPTT Users identified independently of transport or network type.

Parameter	Description
MCPTT Group Size	The number of participants per MCPTT group call.
Use CRLF in flow csv	If enabled, it will use the CRLF line terminator in the generated CSV of the configured MCPTT flow. If disabled, it will use LF.

Advanced SIP Settings

The following settings are available under the Advanced SIP Settings section:

- [SIP Custom Headers](#)
- [SIP Authentication](#)

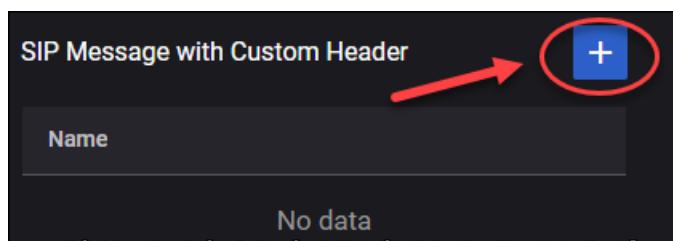
SIP Custom Headers

From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE The message can be deleted by selecting the corresponding **Delete** for each message. Also, you can use the **Edit** button for bulk selection and, then, delete the message in one action.

For each message, you can:

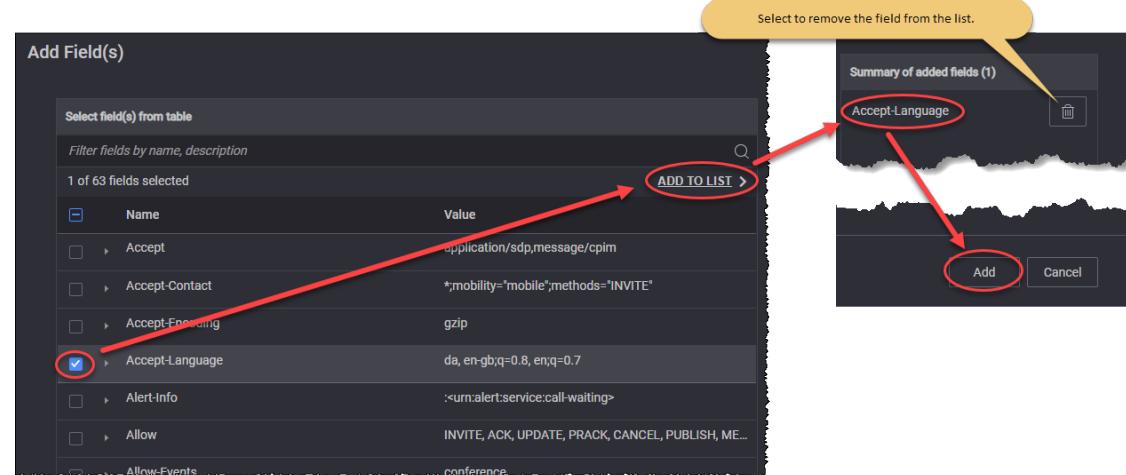
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
 - Select the **Add** button.



The Add Field(s) opens.

- From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



The following custom header are available:

Parameter	Description	Value
Accept	IETF RFC 3261	application/sdp,message/cpim
Accept-Contact	IETF RFC 3841	*;mobility="mobile";methods="INVITE"
Accept-Encoding	IETF RFC 3261	gzip
Accept-Language	IETF RFC 3261	da, en-gb;q=0.8, en;q=0.7
Alert-Info	IETF RFC 3261	:<urn:alert:service:call-waiting>
Allow	IETF RFC 3261	INVITE, ACK, UPDATE, PRACK, CANCEL, PUBLISH, MESSAGE, OPTIONS, SUBSCRIBE, NOTIFY
Allow-Events	IETF RFC 6665	conference
Authentication-Info	IETF RFC 3261, IETF RFC 3310	nexnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	<http://www.example.com/alice/photo.jpg> ;purpose=icon
Content-Disposition	IETF RFC 3261	session

Parameter	Description	Value
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:00 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC 3261	3600
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC	60

Parameter	Description	Value
	4028	
Organization	IETF RFC 3261	Keysight
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC 3327	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>
P-Called-Party-ID	IETF RFC 7315	sip:user1-business@example.com
P-Charging-Function-Addresses	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Charging-Vector	IETF RFC 7315	icid-value=1234bc9876e;icid-generated-at=192.0.6.8;orig- ioi=home1.net
P-Early-Media	IETF RFC 5009	supported
Permission-Missing	IETF RFC 5360	userC@example.com
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com", qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="", stale=False, algorithm=MD5

Parameter	Description	Value
Proxy-Authorization	IETF RFC 3261	Digest username="Alice", realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response ="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>, <sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org?Replaces=425928%40bobster.example.com.3%3Btag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>

Parameter	Description	Value
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

SIP Authentication

The parameters required for SIP authentication are presented in the table below.

Parameter	Description
Username	Provide the username.
Password	Provide the password.
Authentication Type	Select the authentication type: <ul style="list-style-type: none"> • Digest MD5 • AKAv1 • AKAv2 • ProxyDefined

Parameter	Description
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by Cu Isolation, or enter of a K value of your own choosing.
K Increment	The number used to increment the K value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same K value.
Configure OP or OPC	Select the operator-specific authentication value.
Op	The Auth OP value specifies the operator-specific authentication value to use for the UEs in this range. It is a string with a maximum length of 34 characters. It remains fix for all Subscriber/SIM of an operator. You can accept the value generated by Cu Isolation, or enter of an OP value of your own choosing.
Opc	The OPC value is derived from the subscriber key K and the operator dependent value OP. You can accept the value generated by Cu Isolation, or enter of an OP value of your own choosing.
Opc Increment	The number used to increment the OPC value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same OPC value.

DN Video OTT Traffic

The following table describes the Video OTT 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 .
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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 that the computed RTO timer value can be set to.

Parameter	Description
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
<i>TLS Settings</i>	See Server TLS Settings table for more details .

Parameter	Description
OTT Servers	See OTT Servers table for more details.

Server TLS Settings

Parameter	Description
TLSv1.2	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>IMPORTANT Session reuse method is available only if TLSv1.2 is enabled.</p>
Session reuse count	<p>The number of simultaneous connections that can share the same Session ID or Session ticket.</p> <p>IMPORTANT This option appears only if client TLSv1.2 is enabled, and the Session reuse method is set to either the Session ticket or the Session ID method.</p>
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).
Send close notify	If enabled, it will send a close notify message.
TLSv1.3	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.
Certificate file	Select Upload to add your certificate file or Clear to remove it.

Parameter	Description
Key file	Select Upload to add your key file or Clear to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select Upload to add your DH file or Clear to remove it.

OTT Servers

Parameter	Description
	Select this button to add an OTT server to your test configuration.
	Select this button to remove the OTT server from the test configuration.
Server Name	Set the server name. Each server is identified by a unique name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Transport	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/QUIC
Port	Set the port number. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Streams	Refer to Streams for descriptions of the OTT server streams settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Streams

To open the OTT Server Streams panel, select the **Open Streams** button.



The OTT Server Streams parameters are described in the following table.

Parameter	Description
	Select this button to add a stream to your test configuration.
	Select this button to remove the stream from the test configuration.

Parameter	Description
Stream Name	Set the stream name. Each server is identified by a unique name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
URL	Set the URL path.
Type	Select the stream type from the drop-down list: <ul style="list-style-type: none"> • Real • Synthetic
Protocol	Select the protocol from the drop-down list: <ul style="list-style-type: none"> • HLS • DASH. If the stream type is set to Synthetic , you can choose one protocol from list. If the stream type is set to Real , you will see the protocol of real stream loaded.
Stream Duration	If the stream type is set to Synthetic , you can configure the stream duration in seconds. If the stream type is set to Real , you will see the real stream duration.
Segment Duration	If the stream type is set to Synthetic , you can configure the segment duration in seconds. If the stream type is set to Real , you will see the real segment duration.
Quality Levels:	<i>Set the quality value for each level.</i>
	Select this button to add a quality level to your test configuration.
	Select this button to remove the quality level from the test configuration.
Bitrate (kbps)	Set the value of the bitrate.
Resolution	Select the resolution from the drop-down list. Available options: QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K .
Frames per second	Set the number of frames per second.

Custom Parameters/Headers

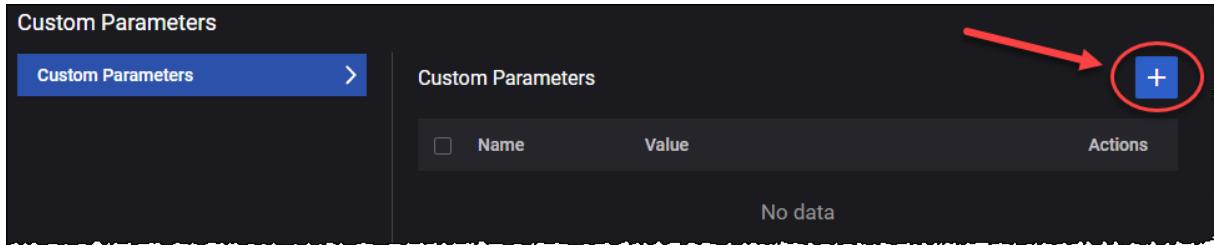
You can add custom parameters as follows:

1. Select the **Open Custom Parameters** button.



The Custom Parameters/Custom Headers panel opens.

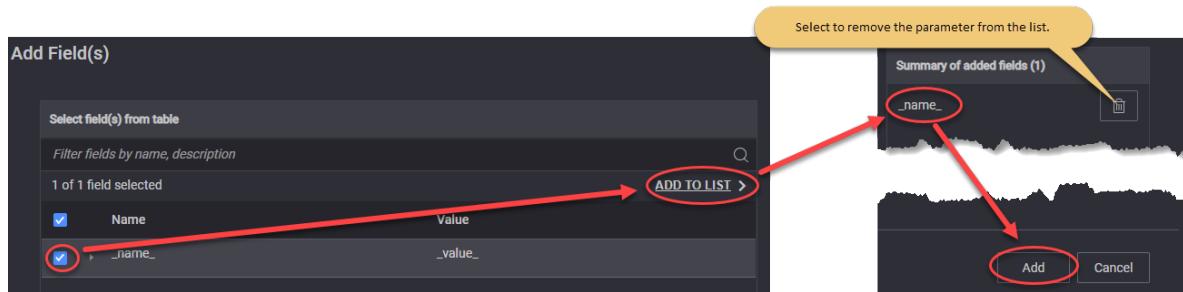
- Select the **Add** button.



The Add Field(s) opens.

- From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



- Once added in the Custom tables, you can edit the value, or press the Menu icon (⋮) to Edit name or Delete the new parameter/header. You can also reorder the items in these tables by dragging them up or down.

DN DNS Server Traffic

The following table describes the DNS Server 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 Server .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
<i>DNS Servers:</i>	
	Select this button to add an DNS server to your test configuration.
	Select this button to remove the DNS server from the test configuration.
Type	Select the type from the available options.
Port	Set the port number. You can accept the value provided by Cu Isolation or

Parameter	Description
	overwrite it with your own value.
Zone Manager	Refer to Zone Manager for descriptions of the DNS server zones settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Zone Manager

To open the DNS Server Zones panel, select the **Open Zones** button.



The DNS Server Zones parameters are described in the following table.

Parameter	Description
+	Select this button to add a zone to your test configuration.
-	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Master Server	Provide the value for the master server.
<i>Resource Records (RRs)</i>	
+	Select this button to add a resource record to your test configuration.
-	Select this button to remove the resource record from the test configuration.
Type	Select the type from the drop-down list. The available options are: <ul style="list-style-type: none"> • A • AAAA
Hostname	Set the hostname.
Address	Provide the address.

Custom Parameters

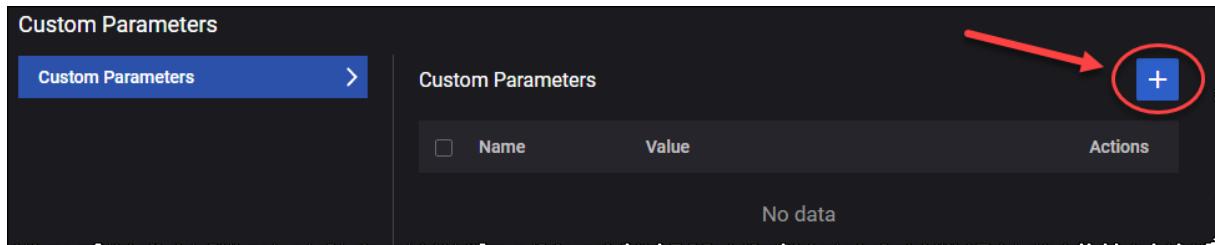
You can add custom parameters as follows:

1. Select the **Open Custom Parameters** button.



The Custom Parameters panel opens.

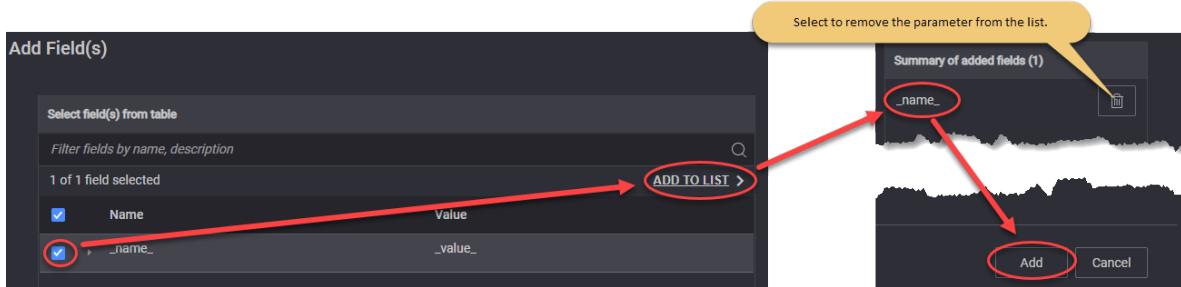
2. Select the **Add** button.



The Add Field(s) opens.

3. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



DN Predefined Applications Traffic

The following table describes the Predefined Applications parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Predefined Traffic Profiles	Select the traffic profile from the available options.

DN Capture Replay

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Capture Replay .

Parameter	Description
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Capture File	It allows you to upload a capture file, using the Upload button. To remove the file, select the Clear button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to 0 for no limit. The default value is 1 .
Maximum Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Limit Maximum Packet per Client	If enabled, it will ensure that, once the limit is reached, no more packets are captured for that DN.
Rx Timeout (ms)	Time the responder waits for packets, after the delay observed in the packet capture. The default value is 1000 milliseconds.
Delayed Tx	Prevent the packets from being sent faster than they appear to be sent in the capture file, trying to maintain the packet delays. The default value is true (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is true (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
Replay Mode	The type of replay mode that will be used on this application traffic. Options are: Ethernet or IP .

The following table describes the Filter object parameters.

Parameter	Description
<i>Filter</i>	
	Select this button to add a new filter to your test configuration.
	Select this button to remove the additional route from your test configuration.
Role	Select the role from the drop-down list. Available options: Initiator and Responder . Default value: Initiator .

Parameter	Description
Filter Expression	This field cannot be empty. It selects the packets to be replayed from uploaded capture. The filter string should be in <code>pcap-filter</code> format, as described at https://www.tcpdump.org/manpages/pcap-filter.7.html .
Remove Encapsulation	Remove GTPu encapsulation from packets, if present, before trying to match the filter expression and when replaying the packets. The default value is false (option disabled).
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

DN Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Synthetic .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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 that the computed RTO timer value can be set to.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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.

Parameter	Description
	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).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).

The following table describes the **Traffic Flow** parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP .
Port	This represents the server(destination) port. This value is editable.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

DN UDG

The following table describes the **UDG** parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to UDG .
Label	Set the label name. You can accept the value provided by the application or overwrite it with your own value.
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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 that the computed RTO timer value can be set to.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	If necessary, enable this option.

Parameter	Description
<i>UDP Settings</i>	
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).

The following table describes the **Traffic Flow** parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP .
<i>Out of Band Signaling</i>	<i>Select this check-box to enable OOB signaling. More details about the required parameters here.</i>
	IMPORTANT <i>To use the OOB feature, the OOB interface must be set in Agent Management window.</i>
Port	This represents the server(destination) port. This value is editable.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

The following table describes the **Out of Band Signaling** parameters.

Parameter	Description
Local Address	The local IP address.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC Address	Hardware MAC address.

Parameter	Description
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Remote Address	The remote IP address.
Port	Set the used port.

DN Throttling settings

Throttling can be enabled from this menu per DN range (by selecting the corresponding check box), and matching user plane traffic over TCP, UDP or both.

Throttling can be useful, for example, when the local network interface that is generating downlink traffic has a higher speed than the radio interface between the UE and the GNB. If the traffic generated from either direction is bursty, the throttling mechanism will, instead of dropping packets, add them in a queue and spread them throughout a second according to the configured bit rate.

NOTE

The throttling options only work for interfaces that are running IxStack, either over DPDK or over raw sockets, depending on where the traffic is terminated (if agent is present on DN/SGi server then its N6 interface should be IxStack; if there is no agent on DN/SGi, than N3 interface should be IxStack on UPF/CoreSim agent).

The following table describes the **Throttling Settings** that you can configure for each DN range.

Settings	Description
Bit Rate (mbps)	Can be set between 10 and 10000. Represents the value at which the traffic will be throttled, and it will become the enforced maximum bit rate.
Throttle TCP Traffic	Select the check box to throttle UP traffic over TCP.
Throttle UDP Traffic	Select the check box to throttle UP traffic over UDP.

CHAPTER 15

UE configuration settings

When you select the **UE** object from the topology window, Cu Isolation 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.

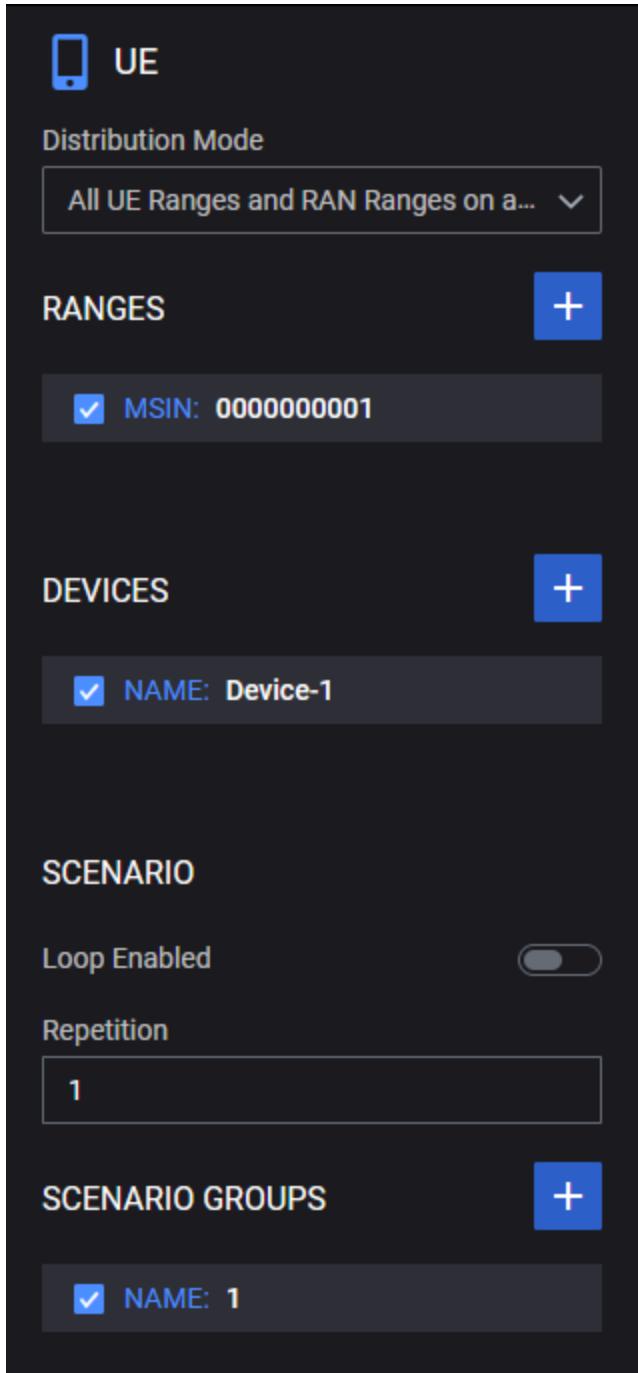
The topics in this chapter describe the configuration settings. For procedural instructions, refer to [Configure UEs on page 38](#).

Chapter contents:

UE panel	224
UE RANGE settings	226
Identification settings	228
UE Security settings	228
UE ESM settings	230
UE EMM settings	232
UE NR Provisioning	234
UE Core Settings	235
Subscribed AMBR settings	247
UE DNNs Config	247
SMS Configuration	250
Untrusted WiFi Settings	251
Network Slicing settings	254
UE NSSAI settings	254
UDM SNSSAI Mappings	255
UE Device settings	257

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.

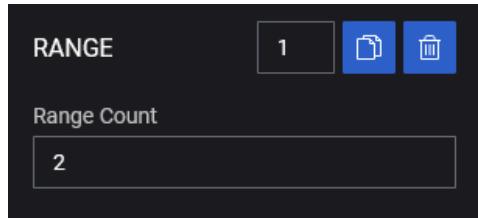
Scenario Groups

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](#)
- [UE Device settings on page 257](#)
- [UE Test Objective settings on page 259](#)
- [Scenario and Scenarion Groups settings on page 334](#)

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
Number of Copies	You can create multiple identical ranges by inserting the number of copies to be created.
	Select the Copy button to create the duplicated ranges.
	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 257) 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 and Scenarios Groups settings for detailed information.
Range settings	Configure detailed UE range settings: <ul style="list-style-type: none"> • Identification settings • UE Security settings • UE ESM settings • UE EMM settings • UE NR Provisioning • UE Core Settings • Subscribed AMBR settings • UE DNNs Config • SMS Configuration • Untrusted WiFi Settings on page 251
Network Slicing	Configure network slicing for this range of UEs: Network Slicing settings .

Setting	Description
Objectives	Configure objectives for this range of UEs: UE Test Objective settings .

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.
IMEI	The first International Mobile Equipment Identity (IMEI) number to assign in this range of UEs.
IMEI Increment	The increment value to create a unique IMEI for each UE in a range.
Software Version	The two-digit software version (SV) number that will be appended to the IMEI to generate the IMEISV value.

UE Security settings

Each UE range requires security settings for subscriber authentication and subscriber privacy. 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.

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 reveal the SUCI.

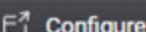
For detailed information, refer to 3GPP TS 33.501 (Security architecture and procedures for 5G System). The following table describes the UE Security Settings.

Setting	Description
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by CuSIM or enter of a K value of your own choosing.
Configure OP or OPC	Select the operator-specific authentication value.
OP	The Auth OP value specifies the operator-specific authentication value to use for the UEs in this range. It is a string with a maximum length of 34 characters. It remains fix for all Subscriber/SIM of an operator. You can accept the value generated by CuSIM or enter of an OP value of your own choosing
OPC	The OPC value is derived from the subscriber key K and the operator dependent value OP. You can accept the value generated by CuSIM or enter of an OP value of your own choosing.
RAND	A hexadecimal number that represents the 128-bit random challenge. You can accept the value generated by CuSIM or enter of a RAND value of your own choosing.
AUTN	The AUthentication TokeN (AUTN) to use when authenticating the UEs in this range.

UE 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	<p> Configure</p> <p>Click the Configure button if you need to configure Protocol Configuration Options (PCOs) for this Subscriber range. Cu Isolation will open the floating Protocol Configuration Options dialog in which you will configure the PCOs (refer to Protocol Configuration Options dialog on the facing 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, Cu Isolation 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.

UE 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	Select the Attach Type value for the Attach procedures that the subscribers in the range will request. <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	Select the type of Detach procedure that the subscribers in the range will request. <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	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.
Extended Periodic Timers Supported	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.
Enable Timer 3412 extended value	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. 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.
Timer 3412 extended value	Enter the Timer 3412 extended value. This is an integer in the range 0-31. 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.
Attach Without PDN	When this option is enabled, the UE specifies—in the Preferred Network Behaviour indication—that Attach Without PDN Connectivity is supported.

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-HSN, starting from the UE identity. The default algorithm is CRC-32. The other option is crc32-bzip2.

UE 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. 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 border="1"> <thead> <tr> <th>Scheme</th> <th>Identifier</th> <th>Size of the scheme output</th> </tr> </thead> <tbody> <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> </tbody> </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.													

UE Core Settings

Each UE range has a set of **Settings** that configure subscription data and PDU session data for the range.

Setting	Description
<i>Settings:</i>	
Dual Registration Mode	When enabled, this option allows an UE to be registered/attached to EPS and 5GS Networks simultaneously.
Allow MICO Mode	This option, when selected, indicates that the UEs in the range prefer Mobile Initiated Connection Only (MICO) mode during Initial Registration and Registration Update procedures.
Subscribed Registration Timer (s)	The Periodic Registration timer value for this range of UEs. The AMF allocates a periodic registration timer value to the UE based on local policies, subscription information and information provided by the UE. After the expiry of this timer, the UE performs a periodic registration.
Active Time (s)	The subscribed Active Time for Power Saving Mode (PSM) UEs.
RAT Restrictions	UE Mobility Restrictions include RAT restrictions, which define the 3GPP Radio Access Technologies (one or more) that a UE is not allowed to access in a PLMN. The options available in Cu Isolation are: NR, E-UTRA, WLAN, and Virtual.
Set ESM Information Transfer Flag	By default, this option is enabled. This option controls the value of the <i>ESM information transfer</i> flag from InitialUEMessage/AttachRequest 4G message. When this option is disabled, the UE/eNodeB will set the flag <i>ESM information transfer</i> to <i>False</i> and MME will not send DonwlinkNASTransport/ESM information request.
Switch Off Deregistration/Detach	When this option is enabled, the Deregistration Request/Detach messages will use a deregistration/detach type of Switch-off. When the Deregistration/Detach type is switch-off, the AMF/MME does not send the Deregistration/Detach Accept message back to the UE.
PDU Session Release Before Deregistration	When this option is enabled, the UE will release PDU sessions before deregistration.
Enable Periodic Registration Update/Periodic Tracking Area Update	By default, this option is not enabled. If the periodic registration / TAU functionality is disabled, the UE will ignore the T3512/T3412 timer received in the Registration Accept/TAU Accept and will not send any Periodic Registration Update/Tracking Area Update request.

Setting	Description
	<p>During the Initial Registration/Initial Attach, the AMF/MME sends in the Registration Accept/Attach Accept a T3512/T3412 timer, which consists of a Unit-Value pair. For example, a value of 30 and unit of 10min means 300 minutes.</p> <p>The T3512/T3412 timer can be overridden by subsequent Registration Accept/TAU Accept messages. If T3512/T3412 is 0 or Disabled, no periodic registration/periodic TAU should be performed. If no T3512/T3412 value is present in the Registration Accept /Attach Accept message, the last known T3512/T3412 value is used. If a T3512/T3412 was never transmitted by the AMF/MME, the default value of 54 minutes will be used.</p> <p>The T3512/T3412 timer is triggered when the UE enters idle. If the UE exits the idle state, the T3512/T3412 timer is stopped. When the UE enters again in idle, the T3512/T3412 timer is restarted.</p> <p>While the UE is in idle mode, when the T3512/T3412 timer expires:</p> <ul style="list-style-type: none"> • If the UE is not registered/attached for emergency services, the UE initiates a Periodic Registration Update/Tracking Area Update procedure and restarts the T3512/T3412 timer. • If the UE is registered/attached for emergency services, the UE locally de-registers/detaches and the AMF/MME locally detaches the UE.
Delay Before PDU Session Creation (ms)	The time that will elapse before the UEs in this range begin creating PDU sessions after successful Registration.
Delay Before Deregister (ms)	The time that will elapse between PDU Session Release Complete and UE initiated Deregistration Request messages.
Delay Before Handover Notify (ms)	The time to wait before handover notification.
Delay before paging (s)	The time to wait before paging, after UE enters idle.
Paging Storm Iterations	The number of times the UE will be paged.
Paging Storm Interval (ms)	The delay between paging messages, in milliseconds.
Check AUTN	<p>By default, this option is disabled.</p> <p>When the option is enabled, then UE will check the value of AUTN in the <i>Authentication Request</i> messages and it will reply with <i>Authentication Failure (MAC failure)</i> in case of different MAC values or with <i>Authentication Failure (Synch failure)</i> in the case the sequence number computed using the AUTN value is invalid.</p>
Unsolicited Router Advertisement	Select to enable this option.

Setting	Description
AMF Force Identification During Registration	This option will force the AMF to always trigger the Identification Procedure to get the identity of the UE. When the NG-RAN node receives this request, it responds with the IMEISV or the SUCI.
IP Address Increment	Set the IP address increment value.
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> • SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. • SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) 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 in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Identity Request PEI Type	<p>When the Identification Procedure is triggered by the MME/AMF due to the AMF Force Identification During Registration option being enabled, it allows the selection of the requested PEI type: IMEISV or IMEI.</p> <p>Default value: IMEISV.</p>
Send Registration Accept in Initial Context Setup Request	If enabled, the UE will send Registration Accept in Initial Context Setup Request.
Always Include Uplink Data Status IE in Service Request Message	The UE will always include the Uplink Data Status IE for a Service Request message, not only if it has pending data.
Enable Passthrough	<p>Select this option to enable passthrough and any interface.</p> <p>Applicable to all passthrough topologies (UE/gNB or UPF).</p> <p>Applicable to either direction: GTPu to IP or/and IP to GTPu.</p>
Attach/Register with GUTI	When the Primary Objective type is Subscribers Per Second, enabling this option will trigger a Registration/Attach Request with the type of user identity set to temporary identity (GUTI). When option is not enabled, the type of user identity in the Registration/Attach Request will be permanent identity.
Authentication with	This option is available only when <i>Attach/Register with GUTI</i> option is

Setting	Description
GUTI	<p>enabled.</p> <p>When enabled, this option triggers authentication in case of attach (4G) / register (5G) with GUTI.</p>
Force Emergency Registration	<p>When this option is enabled, the UE will perform an Emergency registration (instead of Initial Registration).</p> <p>Only the primary objective's DNNs are taken into account when deciding if the UE performs an emergency registration. When the <code>dnnIdsToActivate</code> is present but empty in the primary objective, the Emergency Registration will not be performed even if there is a Secondary Objective that uses an emergency DNN.</p>
Identity Type for Emergency Registration	<p>Select the identity type to use from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> • SUCI/IMSI - where SUCI is used for 5G network, and IMSI for 4G network • IMEISV/IMEI - where IMEISV is used for 5G network, and IMEI for 4G network.
Support SMS	<p>When this is selected, a flag will be added in the Registration message advertising UE support for SMS over NAS feature.</p>
Delay Before Indirect Forwarding Cleanup (ms)	<p>The time that will elapse before indirect forwarding cleanup. The delay is calculated from the UE Context Release.</p>
Send Native GUTI During IRAT Mobility Registration	<p>Enable this option to send native GUTI during IRAT mobility registration.</p>
Authentication During Mobility Registration	<p>Select a value from the drop-down list:</p> <ul style="list-style-type: none"> • Never: Authentication is not performed during mobility registration. • Always: Authentication during mobility registration is always performed. • No Native Context: Authentication during mobility registration is performed only when the UE does not hold a native 5G security context.
Update GUTI in TAU	<p>Select to enable this option.</p>
Access Class	<p>Select the Access Class of the UE from the drop-down list. The following options are available: <i>None</i>, <i>Low Priority Access</i>, <i>11 - For PLMN Use</i>, <i>12 - Security Service</i>, <i>13 - Public Utilities</i>, <i>14 - Emergency Services</i>, <i>15 - PLMN Staff</i>.</p> <p>IMPORTANT This option is available for 4G only.</p>

Setting	Description
<i>Radio Capability</i>	
UE Radio Capability IE Value for LTE	The UE radio capability IE value that will be included UE Capability Info Indication message.
UE Radio Capability IE Value for NR	The UE radio capability IE value that will be included UE Capability Info Indication message.
<i>Send UE Capability IE Indication after Initial Context Setup</i>	Enable this option to send UE capability IE indication after initial context setup.
Replay UE Radio Capability	<p>The UE Radio Capability IE is replayed in the Initial Context Setup Request and UE Radio Capability Match / Check messages on 4G and 5G. This option is applicable for the AMF and MME nodes.</p> <p>NOTE It is not applicable for Initial Context Setup Request of an inter-RAT handover procedure.</p> <p>NOTE After UE Radio Capability Match / UE Radio Capability Check procedures, UE always sends UE Radio Capability Info Indication.</p>
<i>Handover</i>	<i>Select the check box to enable this option.</i>
<i>Report Interval</i>	Select from the drop-down the time interval between successive event notifications.
<i>Report Amount</i>	Select from the drop-down the number of measurement reports that the UE sends to the network before stopping.
<i>Event A3</i>	
A3 Offset RSRP	The value configured will define the difference in signal quality between the serving and neighboring cells.
Hysteresis	Define a margin above or below the A3 Event Offset that must be exceeded before the event is triggered or canceled.
Time to Trigger	Select from the drop-down the time during which specific criteria for the event has to be met in order to trigger a measurement report.
<i>Location Reporting</i>	<i>Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).</i>
<i>Reporting Type</i>	<p>Select the value from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • Direct - If the test timeline is long enough, the AMF generates n LocationReportingControl messages at every m seconds from the moment Registration Complete message is received by the AMF (n is the value configured for Number of Repeats and m is the value of Interval Between Requests).

Setting	Description
	<ul style="list-style-type: none"> • Change of Serving Cell - In case of Handover with AMF change, if Change of Serving Cell is selected, after handover, the new AMF will send a <code>LocationReportingControl</code> message to the NG-RAN.
Interval Between Requests (seconds)	Set the time interval between requests.
Number of Repeats	Set the number of repeats.
Start Time (seconds)	The number of seconds after successful attach when the AMF sends a <code>LocationReportingControl</code> message (event-type: <code>change-of-serving-cell</code>).
Stop Time (Seconds)	The number of seconds since the <u>Start Time</u> when the AMF sends <code>LocationReportingControl</code> message (event-type: <code>stop-change-serving-cell</code>).
<i>SMF Initiated PDU Session Release</i>	<i>Select the check box to enable this option.</i>
Time to Wait before SMF Initiated PDU Session Release (s)	Time in seconds to wait before SMF initiated PDU session release.
DNNs	<p>Select the DNNs from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list.
<i>Network Initiated Deregistration</i>	<i>Select the check box to enable this option.</i>
Time to wait before Network Initiated Deregistration (s)	Time in seconds to wait before network initiated deregistration.
Set Reregistration Required Flag in Deregistration Request Message	Enable this option to set a required reregistration flag in the deregistration request message.
<i>AMF Initiated UE Context Release</i>	<i>Select the check box to enable this option.</i>
Time to Wait before AMF Initiated UE Context	Time in seconds to wait before AMF initiated UE context release.

Setting	Description
Release (s)	
<i>Location Services</i>	<p>Select the check box to enable Location Services (as described in TS23271/23273). The Location Services procedures over the LPPa /NRPPa interface are detailed in TS36455/38455.</p> <p>NOTE When Location Services is enabled, at least 1 profile must be configured (a maximum of 15 profiles allowed).</p>
Reroute NAS Request	Select the check box to enable this option.
AMF Set ID	The AMF Set ID to use for this simulated AMF node. The Set ID uniquely identifies the AMF Set within the AMF Region.
Reroute After SMC	If selected, the AMF will reroute after Security Mode procedure.
NSSAI	See the NSSAI table for details.
<i>Network Initiated PDU Session Modification</i>	See the Network Initiated PDU Session Modification on page 244 table for details.
Refresh Security Context	When enabled, the AMF will initiate the Security Mode Control procedure to obtain a fresh uplink NAS Count which is used to generate a new Security Key.
Delay(s)	The time to wait, in seconds, before triggering the Security Mode Control procedure after the UE is registered.
Iterations	The number of times the security context will be refreshed.
Interval(s)	The time, in seconds, between two iterations.
<i>Core Network Assistance Information For Inactive</i>	<p>If enabled, the configured Core Network Assistance Information for RRC INACTIVE IE is present only in the INITIAL CONTEXT SETUP REQUEST message carrying the initial Registration Accept. It is not present in the INITIAL CONTEXT SETUP REQUESTS carrying other types of NAS messages, UE CONTEXT MODIFICATION REQUEST, HANDOVER REQUEST or PATH SWITCH REQUEST ACKNOWLEDGE. It is not present for Emergency Registration.</p> <p>This option is disabled by default.</p>
UE Specific DRX	<p>The UE Specific DRX value can be selected from the available options:</p> <ul style="list-style-type: none"> • DRX32 • DRX64 (default value) • DRX128 • DRX256 • None - if selected, this IE will not be included in the message

Setting	Description
Paging Throttling	
Throttling Criterion	Select the criterion on which two consecutive Paging messages triggered by the downlink traffic should be sent: <ul style="list-style-type: none"> • Seconds • Packets
Value	Assign a number of seconds to wait, or packets to skip until Paging is sent again. A value of 0 disables this option.

Location Services

The following table describes the **Location Services** settings.

Setting	Description
<i>Location Services:</i>	
	Select the Add LCS Profile button to add a new profile.
	Select the Delete LCS Profile button to remove the profile from your test configuration.
Trigger	Select an option from the drop-down list: <ul style="list-style-type: none"> • None - no trigger (default option). • UE Available - UE exits Idle mode. • Change of Area - UE performs handover with TAC change.
<i>E-CID Measurements:</i>	
	Select the Add E-CID Measurements button to add a new measurement. <p>IMPORTANT A maximum of 15 E-CID Measurements can be configured across all LCS Profiles for an UE range.</p>
	Select the Delete E-CID Measurements button to delete the measurement from your test configuration.
Report Characteristics	Select an option from the drop-down list: <ul style="list-style-type: none"> • On Demand - information is needed on demand in real time. • Periodic - periodic E-CID measurement reports.
Measurement Quantities	Select an option (or more) from the drop-down list. The available options are: Cell-ID (default), Angle of Arrival , Timing Advance Type 1 , Timing Advance Type 2 , RSRP , RSRQ . The following measurement quantities become available as follows:

Setting	Description
	<ul style="list-style-type: none"> SS-RSRP, SS-RSRQ, CSI-RSRP, CSI-RSRQ, Angle of Arrival NR - for 5G only, when <i>Technical Spec Version</i> is set to either R16 September 2020, or R17 December 2022 (see Global Settings). Timing Advance NR - for 5G only, when <i>Technical Spec Version</i> is set to R17 December 2022. <p>NOTE There is no support for Inter-RAT Measurement Quantities and WLAN Measurement Quantities.</p>
Delay (ms)	<p>This option is available only when the <i>Trigger</i> is set to None. It represents the time trigger for E-CID measurement initiation.</p>
Periodicity	<p>This option is available only when the <i>Report Characteristics</i> is set to Periodic. It represents the periodicity of E-CID measurement reports. The available options are: 120 ms, 240 ms, 480 ms, 640 ms, 1024 ms, 2048 ms, 5120 ms, 10240 ms, 1 min, 6 min, 12 min, 30 min, 60 min.</p>
Duration (ms)	<p>This option is available only when the <i>Report Characteristics</i> is set to Periodic. It represents the timer to trigger E-CID measurement termination.</p>

5G Location Services Release 16 specific additions are not supported:

- LMF UE Measurement ID in E-CID MEASUREMENT messages doesn't support (1 ... 256) values, supporting (1 ... 15) instead.
- RAN UE Measurement ID in E-CID MEASUREMENT messages doesn't support (1 ... 256) values, supporting (1 ... 15) instead.
- Measurement Periodicity in E-CID MEASUREMENT messages doesn't support 20480ms, 40960ms values.
- Measurement Quantities in E-CID MEASUREMENT messages doesn't support SS-RSRP, SS-RSRQ, CSI-RSRP, CSI-RSRQ, NR Angle of Arrival values.

5G Location Services LPPa/NRPPa Routing ID values in DOWNLINK/UPLINK UE ASSOCIATED LPPa/NRPPA TRANSPORT messages are hardcoded to **0**.

NSSAI

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

Setting	Description
NSSAI:	
	Select the Add UE NSSAI button to add a new UE NSSAI to your test configuration.
NSSAI Settings:	

Setting	Description								
	Select the Delete UE NSSAI button to delete this UE NSSAI from your test configuration.								
SST	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: <table border="1" data-bbox="344 481 1437 713"> <thead> <tr> <th>SST</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>eMBB</td> <td>1</td> </tr> <tr> <td>URLCC</td> <td>2</td> </tr> <tr> <td>MIoT</td> <td>3</td> </tr> </tbody> </table>	SST	Value	eMBB	1	URLCC	2	MIoT	3
SST	Value								
eMBB	1								
URLCC	2								
MIoT	3								
SD	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.								
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.								

Network Initiated PDU Session Modification

The following table describes the **Network Initiated PDU Session Modification** settings.

Setting	Description
<i>Network Initiated PDU Session Modification:</i>	
	From the panel, you can select a DNN Config for editing and also add additional DNN configurations. Select the Add DNNs Config button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the Delete DNN Config button to delete this DNN config from your test configuration.
DNN	From the drop-down, select one of the previously-defined DNNs.
Delay Before Network Initiated PDU Session Modification (s)	The time to wait, in seconds, between the PDU Session Establishment end and the start of Network Initiated PDU Session Modification procedure start.

Setting	Description
Interval Between Consecutive Network Initiated PDU Session Modification procedures (s)	The time, in seconds, between two Consecutive Network Initiated PDU Session Modification procedures.
Iterations	The number of consecutive Network Initiated PDU Session Modification procedures per UE.
<i>Flows:</i>	<i>This option lists all the flows defined and associated to the selected DNN. Select the check-box to configure a flow. By default, the default bearer is selected.</i>
	Select the Add Flow button to add a new flow to your test configuration.
<i>Flow:</i>	
	Select the Delete Flow button to delete this DNN config from your test configuration.
Flow ID	Select the flow's ID from the drop-down list.
ARP	<i>If enabled, the Allocation and Retention Priority (ARP) setting specifies the priority level, preemption capability, and preemption vulnerability of a resource request.</i>
ARP Priority Level	<p>Specify the ARP priority level.</p> <p>The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by home network and thus applicable when a UE is roaming.</p>
ARP Preemption Capability	<p>The available options are:</p> <ul style="list-style-type: none"> • Not Preempt • May Preempt - if selected, the packets in this Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.
ARP Preemption Vulnerability	<p>The available options are:</p> <ul style="list-style-type: none"> • Not Preemptable • Premptable - if selected, the packets in this QoS Flow are candidates for being preempted by other flows. When a flow is preemption-vulnerable, it

Setting	Description																				
	can be dropped to free up resources for packets that have a higher ARP priority level.																				
<i>GBR</i>	<i>If enabled, configure the parameters to indicate the guaranteed bit rates (GBR) for the selected flow.</i>																				
GBR Type	Select the desired guaranteed bit rate (GBR) type for the flow. Based on your selection, Cu Isolation will show the appropriate settings to configure. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2"><i>QoS Rates:</i></td></tr> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>Uplink</td><td>Set the uplink bitrate.</td></tr> <tr> <td>Downlink</td><td>Set the downlink bitrate.</td></tr> <tr> <td colspan="2"><i>Dynamic QoS Rates:</i></td></tr> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>Uplink Action</td><td>Select the action type to apply to the uplink bitrate.</td></tr> <tr> <td>Uplink Step</td><td>Select the step to increase or decrease the uplink bitrate.</td></tr> <tr> <td>Downlink Action</td><td>Select the action type to apply to the downlink bitrate.</td></tr> <tr> <td>Downlink Step</td><td>Select the step to increase or decrease the downlink bitrate.</td></tr> </table>	<i>QoS Rates:</i>		Parameter	Description	Uplink	Set the uplink bitrate.	Downlink	Set the downlink bitrate.	<i>Dynamic QoS Rates:</i>		Parameter	Description	Uplink Action	Select the action type to apply to the uplink bitrate.	Uplink Step	Select the step to increase or decrease the uplink bitrate.	Downlink Action	Select the action type to apply to the downlink bitrate.	Downlink Step	Select the step to increase or decrease the downlink bitrate.
<i>QoS Rates:</i>																					
Parameter	Description																				
Uplink	Set the uplink bitrate.																				
Downlink	Set the downlink bitrate.																				
<i>Dynamic QoS Rates:</i>																					
Parameter	Description																				
Uplink Action	Select the action type to apply to the uplink bitrate.																				
Uplink Step	Select the step to increase or decrease the uplink bitrate.																				
Downlink Action	Select the action type to apply to the downlink bitrate.																				
Downlink Step	Select the step to increase or decrease the downlink bitrate.																				
<i>MBR</i>	<i>If enabled, configure the maximum bit rates (MBR) allowed for the selected flos.</i>																				
MBR Type	Select the desired maximum bit rate (MBR) type for the flow. Based on your selection, Cu Isolation will show the appropriate settings to configure. <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2"><i>QoS Rates:</i></td></tr> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>Uplink</td><td>Set the uplink bitrate.</td></tr> <tr> <td>Downlink</td><td>Set the downlink bitrate.</td></tr> <tr> <td colspan="2"><i>Dynamic QoS Rates:</i></td></tr> <tr> <th>Parameter</th><th>Description</th></tr> <tr> <td>Uplink Action</td><td>Select the action type to apply to the uplink bitrate.</td></tr> <tr> <td>Uplink Step</td><td>Select the step to increase or decrease the uplink bitrate.</td></tr> <tr> <td>Downlink Action</td><td>Select the action type to apply to the downlink bitrate.</td></tr> </table>	<i>QoS Rates:</i>		Parameter	Description	Uplink	Set the uplink bitrate.	Downlink	Set the downlink bitrate.	<i>Dynamic QoS Rates:</i>		Parameter	Description	Uplink Action	Select the action type to apply to the uplink bitrate.	Uplink Step	Select the step to increase or decrease the uplink bitrate.	Downlink Action	Select the action type to apply to the downlink bitrate.		
<i>QoS Rates:</i>																					
Parameter	Description																				
Uplink	Set the uplink bitrate.																				
Downlink	Set the downlink bitrate.																				
<i>Dynamic QoS Rates:</i>																					
Parameter	Description																				
Uplink Action	Select the action type to apply to the uplink bitrate.																				
Uplink Step	Select the step to increase or decrease the uplink bitrate.																				
Downlink Action	Select the action type to apply to the downlink bitrate.																				

Setting	Description	
	Downlink Step	Select the step to increase or decrease the downlink bitrate.

Subscribed AMBR settings

The following tables describes the Subscribed AMBR configuration settings.

Parameter	Description
Subscribed AMBR Uplink	The subscribed uplink Session-AMBR value for this UE range. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.
Subscribed AMBR Uplink unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Subscribed AMBR Downlink	The subscribed downlink Session-AMBR value for this UE range. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.
Subscribed AMBR Downlink unit	The unit in which the rate is expressed. The options range from bps to Tbps.

UE DNNs Config

You use the DNNs Config panel to configure one or more Data Network Names (DNNs) for each UE range. These settings establish a mapping between DNNs and UE IPs, thereby enabling multiple PDU sessions for each UE in the range.

The following table describes the UE **DNNs Config** settings.

Setting	Description
<i>DNNs Config:</i>	
	From the panel, you can select a DNN Config for editing and also add addition DNN configurations. Select the Add DNNs Config button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the Delete DNN Config button to delete this DNN config from your test configuration.

Setting	Description
SSC Mode	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> • SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. • SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) 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 in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Session ID	Provide the session ID value.
Deactivation Delay (s)	Delay measured from PDU Session Establishment until CN initiated selective deactivation of the User Plane connection.
Reactivation Delay (s)	Delay measured from CN initiated selective deactivation of a User Plane connection until UE initiated reactivation (Service Request in CM-Connected Mode).
DNN	Select one of the previously-defined DNNs from the drop-down list.
Local IPv4 Address	<p>The IPv4 address that the UE receives from the SMF during PDU Session Establishment. This address is used for L4-7 traffic (source IP for the UL traffic, destination IP for the DL traffic).</p> <p>IP address is also used to create UE Routes from DN.</p>
Local IPv4 Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Local IPv4 Address Increment	The value by which the IP addresses will be incremented.
Configure S-NSSAI:	<p><i>When this check-box is selected, you can configure which slice (S-NSSAI) to be send in PDU Session Establishment messages. If the check-box is not selected, the first slice from Allowed NSSAI list (received in Registration Accept) is used in PDU Session Establishment message.</i></p> <p style="text-align: center;">NOTE <i>This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</i></p>
S-NSSAI	This list contains all the slices defined for the selected UE range. Select from the drop-down list the slice to be used in PDU Session Establishment.

Setting	Description
Force S-NSSAI	<p>This option is used to control the behavior in case you select a slice that is not part of Allowed NSSAI received from AMF, as follows:</p> <ul style="list-style-type: none"> if the check-box is not selected, the UE will not send any slice in PDU Session Establishment message (as the slice selected from the above list is not part of Allowed NSSAI). if the check-box is selected, the UE will use the slice selected from the above list, although it is not part of Allowed NSSAI. <p>This option is for negative testing purposes, and it is expected the PDU Session Establishment to fail as it uses a slice that is not allowed.</p>
<i>Secondary Authentication:</i>	
Method type	<p>The following options are available:</p> <ul style="list-style-type: none"> None EAP-TTLS (Extensible Authentication Protocol – Tunnelled Transport Layer Security) CHAP (Challenge-Handshake Authentication Protocol) PAP (password Authentication Protocol)
<i>EAP-TTLS Auth Method:</i>	
CA Certificate	Provide the client certificate.
Tunneled Authentication Method	Select the tunneled authentication method: <ul style="list-style-type: none"> PAP CHAP
User	Provide the user.
Password	Provide the password.
Send User Identity	<p>By default, this option is disabled.</p> <p>Enabling this option will add SM PDU DN Request Container IE (Authentication Identity) to the PDU Session Establishment Request message send by NG-RAN.</p>
<i>Chap Auth Method:</i>	
User	Provide the user.
Secret	Provide the password.
<i>PAP Auth Method:</i>	
User	Provide the user.
Password	Provide the password.

SMS Configuration

The following table describes the UE **SMS Configuration** settings.

Setting	Description
<i>Mobile Settings:</i>	
Service Center Address	The service center address used by the UE range for SMS messaging.
Type of Number	<p>The type of number can be one of the following:</p> <ul style="list-style-type: none"> • Unknown • International number • National number • Network specific number • Subscriber number • Alphanumeric • Abbreviated number
Numbering Plan Identification	<p>The numbering plan identification can be one of the following:</p> <ul style="list-style-type: none"> • Unknown • ISDN • Data numbering plan • Telex numbering plan • National numbering plan • Private numbering plan • ERMES numbering plan
Character Set	The character set used in the data coding scheme for the text message.
Text Message	The content of text message sent by the UE via SMS.

Untrusted WiFi Settings

The following table describes the UE **Untrusted WiFi Settings** settings.

Setting	Description
Remote N3IWF	Select the remote N3IWF range from drop-down list.
Destination Port	Read-only field. Value set to 500 .
Source Port	Provide the source port. By default, set to 500 .
Enable NAT-T	Select to enable the NAT Traversal keepalive.
NAS IP Type	Select the NAS IP type from the drop-down list: IPv4 (default) or IPv6 .
Configure a CA Certificate	<p>By default this option is disabled.</p> <p>When enabled, the CA Certificate drop-down is displayed which allows the selection of one of the CA Certificates defined in global settings.</p>
CA Certificate	<p>IMPORTANT This parameter appears only if Configure a CA Certificate is enabled.</p> <p>Select the CA Certificate from the drop-down list.</p>
<i>IKE Phase 1</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. • If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	Select an option from the drop-down list. Available options are: modp768(1), modp1024(2), modp1536(5), modp2048(14), modp3072(15), modp4096(16), modp6144(17), modp8192(18), prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25, secp224r1(26), x25519(31), x448(32) .

Setting	Description
	Default value: prime256v1(19) .
PRF Algorithm	Select an option from the drop-down list. Default value: HMAC-SHA256 . Available options: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 .
<i>IKE Phase 2</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16 .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: NONE . Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 . Restrictions: <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. • If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	Select an option from the drop-down list. Select an option from the drop-down list. Available options are: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER ASN1 DN, ID_KEY_ID . Default value: ID_FQDN .
Local Identification Value	Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR .
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
IKE Phase 1	Set a value for this parameter.

Setting	Description
(IKE) Lifetime (s)	Default value: 0 (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: 0 (disabled).

Network Slicing settings

A UE may access multiple *network slices* over a single Access Network. A Network Slice is defined within a PLMN and includes the Core Network Control Plane and User Plane Network Functions. In addition, it includes the NG Radio Access Network and/or the N3IWF functions to the non-3GPP Access Network. It functions as a logical end-to-end network that runs on a shared physical infrastructure, capable of providing specific network capabilities and characteristics.

Each UE range requires at least one NSSAI (Network Slice Selection Assistance Information) range.

The **Network Slicing** settings include:

UE NSSAI settings **254**

UDM SNSSAI Mappings **255**

UE NSSAI settings

Each UE range requires at least one NSSAI range.

An NSSAI (Network Slice Selection Assistance Information) is a collection of S-NSSAIs (Single Network Slice Selection Assistance Information). An NSSAI may be a Configured NSSAI, a Requested NSSAI, or an Allowed NSSAI. A maximum of eight S-NSSAIs can be sent in signaling messages between the UE and the Network. The Requested NSSAI signaled by the UE to the network allows 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 NSSAI slices are the ones supported by UE (DNN mapping is done from here also) that will be sent in NAS messages (for example Registration, PDU Session Establishment).

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

Setting	Description
<i>UE NSSAI:</i>	
	Select the Add UE NSSAI button to add a new UE NSSAI to your test configuration.
<i>UE NSSAI settings:</i>	
	Select the Delete UE NSSAI button to delete this UE NSSAI from your test configuration.
SST	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:

Setting	Description	
	SST	Value
	eMBB	1
	URLCC	2
	MIoT	3
SD	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.	
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.	

UDM SNSSAI Mappings

You can add and delete SNSSAI Mappings as required to meet your test objectives.

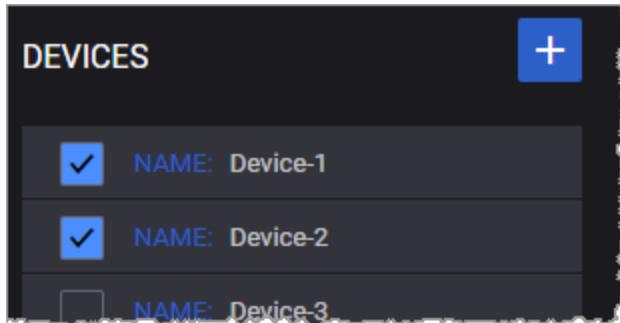
In an Initial Registration or Mobility Registration Update, the UE may include the Mapping Of Requested NSSAI, which is the mapping of each S-NSSAI of the Requested NSSAI to the HPLMN S-NSSAIs. This mapping ensures that the network can verify whether or not the S-NSSAIs in the Requested NSSAI are permitted based on the Subscribed S-NSSAIs.

The following table describes the UE **UDM SNSSAI Mapping** settings.

Setting	Description
<i>UDM SNSSAI Mapping:</i>	
	Select the Add SNSSAI Mapping button to add the NSSAI mapping to your test configuration.
<i>UDM SNSSAI Mapping settings:</i>	
	Select the Delete SNSSAI Mapping button to delete this NSSAI mapping from your test configuration.
SST	The Slice/Service Type (SST) value.
SD	The Slice Differentiator (SD) value for this S-NSSAI.
Mapped SST	The Mapped Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The Mapped Slice Differentiator (SD) value for this S-NSSAI.
DNNS	The Subscription Information for each S-NSSAI may contain a Subscribed DNN list.

Setting	Description
	Select all DNNs required to be activated in this S-NSSAI (via multiple PDU Sessions).

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), Cu Isolation 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](#)

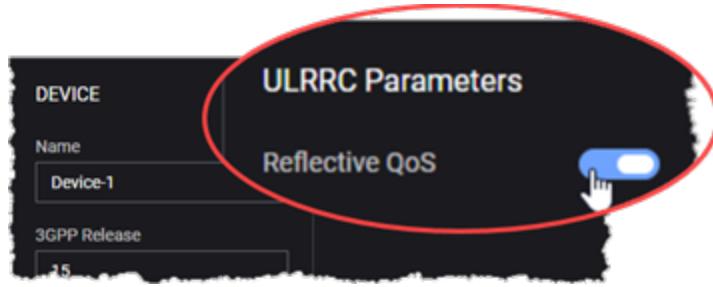
Device settings

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.
<i>UE Additional Capabilities</i>	
NR	This parameter specifies the UE capabilities for NR; it is a hex dump of the encoding of UE capabilities defined for the UE-NRCapability IE in 3GPP TS 38.331.
EUTRA	This parameter specifies the UE capabilities for EUTRA, as defined in UE-EUTRA-Capability IE in 3GPP TS 38.331. The input is in HEX-string format.
EUTRA-NR	This parameter specifies the UE capabilities for EUTRA-NR; it is a hex dump of the encoding of UE capabilities defined for the UEMRDC-Capability IE in 3GPP TS 38.331.

CHAPTER 16

UE Test Objective settings

In a Cu Isolation 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.

Chapter contents:

Control Plane Objective	260
About primary objectives	260
Secondary Control Plane Objective	262
Handover	263
Paging	265
Enter/Exit Idle	266
Create/Delete QoS Flows	266
Create/Delete PDU Sessions	269
SMS	270
User Plane Objectives	271
Stateless UDP Traffic	272
Data Traffic	274
Voice Traffic	280
Video OTT Traffic	296
DNS Client Traffic	301
ICMP Client	304
Capture Replay	304
Synthetic	307
UDG	309
Attacks	314
REST API Client	319
Predefined Applications Traffic	322

Applications	324
Application Advanced Settings	327
TCP Settings	329
TLS Settings	330
RTP Settings	333

Control Plane Objective

You configure Control Plane Objectives for each individual UE range. They are structured as Primary and Secondary objectives. The focus of the primary objectives is on the establishment of subscriber PDU sessions, whereas the focus of the secondary objectives is on the achievement of specific mobile user events during those sessions.

Refer to the following topics for descriptions of the Control Plane Objective settings:

- [About primary objectives](#)
- [Secondary Control Plane Objective](#)

About primary objectives

In the current Cu Isolation release, there are two available primary objectives: *active subscribers* and *subscribers per second*. This topic gives a general description of their respective roles and behaviors.

- [Active Subscribers](#)
- [Subscribers Per Second](#)

Active Subscribers

The active subscribers objective operates over a sequence of three phases: ramp up, sustain, and ramp down. Each of these has its own scope.

Phase	Activity during this phase
Ramp up	Registration + PDU Session Establishment (if enabled via DNNs to Activate option)
Sustain time	Traffic and/or secondary objectives are executed
Ramp down	Delete PDU Session (if enabled) + Dereistration

This can be viewed as a timeline:

|----- Ramp up -----|----- Sustain -----|----- Ramp down -----|

Observations:

- The duration of the ramp up phase is not directly configurable. The ramp up time is automatically computed from the total number of subscribers in the range divided by the configured Ramp-up Rate (`<number_of_subscribers_in_the_range> / <RampUpRate>`). If the ramp up rate cannot be maintained, ramp up will last longer.
- During the sustain time phase, only secondary objectives are running.

- If configured, uplink traffic will start after the ramp up stage is complete.
- Subscribers will accept any downlink traffic once they are attached (registered and PDU session established).
- The duration of ramp down is not directly configurable. The ramp down time is automatically computed from the total number of subscriber in the range divided by the configured Ramp-up Rate ($<\text{number_of_subscribers_in_the_range}> / <\text{RampUpRate}>$).
If the ramp down rate cannot be maintained, ramp down will last longer.
- All User Plane Traffic except Stateless UDP will be started during Ramp Up phase. Stateless UDP traffic starts after all UEs have Registered and Established PDU Sessions.

Example:

Consider a test with 20000 subscribers, configured with an active subscribers objective with a ramp up rate of 1000/s, a secondary objective with a rate of 2000/s, and a sustain time set for 30 seconds. Such a test will give the following results.

<i>Ramp Up Time:</i>	$20000 / 1000 = 20\text{s}$ for subscribers to register
<i>Rate in ramp up time:</i>	1000 registrations per second
<i>Sustain time:</i>	30 seconds
<i>Rate in sustain time:</i>	2000 secondary procedures per second
<i>Ramp down time:</i>	$20000 / 1000 = 20\text{s}$ for subscribers to deregister
<i>Rate in ramp down time:</i>	1000 deregistrations per second

Subscribers Per Second

The Subscribers per Second objective operates over two phases: sustain and ramp down.

Phase	Activity during this phase
Sustain time	All objectives will run: primary objective—both registration and deregistration—and all secondary objectives.
Ramp down	Deregistration will be executed for the UEs that did not complete the hold time during the sustain phase.

This can be viewed as a timeline:

|----- Sustain -----|----- Ramp down -----|

Observations:

- The duration of ramp down is equal to the value of hold time.
- During the ramp down time, only deregistration occurs.

Example:

Consider a test with 20000 subscribers, configured with: a Subscribers per Second primary objective with a rate of 1000/s and a hold time of 10s, a secondary objective with a rate of 2000/s, and a

Sustain time configured for 30 seconds.

Such a test will give the following results.

<i>Sustain time:</i>	30 seconds
<i>Rate in sustain time:</i>	~4000 per second (1000 per second from registration + 1000 per second from deregistration + 2000 per second from secondary objective, because both primary and secondary objective will run at the same time)
<i>Ramp down time:</i>	10 seconds
<i>Rate in ramp down time:</i>	1000 deregistrations per second

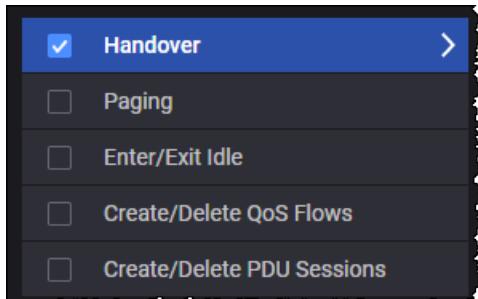
Secondary Control Plane Objective

The focus of the secondary objectives is on the achievement of specific mobile user events during subscriber PDU sessions. For each primary objective that you configure for the UE range, you can select one or multiple Secondary Objectives.

IMPORTANT

The number of UEs must be equal to or greater than the number of secondary objectives configured, in order for all objective procedures to execute. For example, if only one UE is configured and two secondary objectives are configured (such as Handover and Enter/Exit Idle), one of the objectives will be skipped.

In this example, only Handover has been selected:



Note that:

When the primary objective is:	then the secondary objectives will start...
Active Subscribers	after all users are registered.
Subscribers Per Second	at the beginning of the test (immediately after the first user has registered).

Refer to the following topics for descriptions of the Secondary Control Plane objectives:

- [Handover](#)
- [Paging](#)
- [Enter/Exit Idle](#)
- [Create/Delete QoS Flows](#)
- [Create/Delete PDU Sessions](#)
- [SMS](#)

Handover

When you configure a **Handover** secondary objective, each of the active subscribers configured for the primary objective attempts to execute the handover event defined for the objective. During a handover, the UEs in the range are moving amongst a group of NG-RANs. At the start of a handover, the UEs are registered with the Parent NG-RAN (which is configured in the [UE Range panel](#)). The UEs then traverse the NG-RANs that you configure (the *Visited NG-RAN* list).

Handover configuration parameters

The following table describes these objective parameters.

Parameter	Description
<i>Handover:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which handovers are initiated, measured in procedures per second if Distributed over (s) is not modified.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Force N2 Handover	Enable this option to force N2 handover with direct forwarding instead of X2 / Xn handover.
Mobility for State	This option specifies in what state should the UE perform the handover objective. The following options can be selected from the drop-down list: <ul style="list-style-type: none"> • Connected • Idle • Any

Parameter	Description
	When Any is selected, the UE will execute the handover objective, regardless if the UE is in Connected or Idle state.
Force UE State Before Returning to Parent Node	Select an option from the drop down list: <ul style="list-style-type: none"> • None - The UE will perform either Idle Mode Mobility or Connected Handover to parent RAN, depending on what state the UE is before executing the procedure. • Connected - The UE will perform Connected Handover from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in idle state before performing this mobility, the UE will first perform exit idle, and only after the UE is in connected state, will it initiate the connected handover to the parent RAN. • Idle - The UE will perform Idle Mode Mobility from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in connected state before performing this mobility, the UE will first perform enter idle, and only after the UE is in idle state, will it initiate the idle mode mobility to the parent RAN.
Send Service Request after Returning to Parent Node	By default, this option is disabled. Send Service Request immediately after Return to Parent Node Mobility if UE State was idle.
Handover Cancel	<i>When this option is enabled, NG-RAN will trigger a Handover Cancel after receiving Handover Request from AMF. Handover Cancel is applicable only for N2 Handover.</i>
Percentage	The percentage of N2 Handover Procedures that will trigger a Handover Cancel from the gNodeB.
Seed	The seed of Random Number Generator.
<i>Visited gNodeBs/eNodeBs/UNAPs : A list of the NG-RANs that UEs will visit during the test.</i>	
	Add next node to the list.
	Remove the selected node from the list.
Force UE State before Mobility	The following options can be selected from the drop-down list: <ul style="list-style-type: none"> • Connected • Idle • Any
Primary Node	Select the primary node from the drop-down list. If an UNAP is selected as the Primary Node, the Secondary Node field will not be

Parameter	Description
	displayed.
Secondary Node	Select the secondary node from the drop-down list.
Send Service Request After Mobility	By default, this option is disabled. Send Service Request immediately after Mobility if UE State was idle.

Paging

When you configure a **Paging** secondary objective, each of the active subscribers configured for the primary objective attempts to execute the Paging event defined for the objective. Upon receiving a Paging message, each simulated UE—the UEs are in CM-IDLE state—will initiate the UE Triggered Service Request procedure (Reference: 23.502, section 4.2.3.2).

The following table describes the Paging objective parameters.

Parameter	Description
<i>Paging:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Suspend Traffic Interval (s)	The time (in seconds) to suspend traffic on the remote IP address.
Remote IP Address	Set the remote IP address: <ul style="list-style-type: none"> • If the UPF is the DUT in the test topology, then set the <i>Remote IP Address</i> to the DN IP address. • If the UPF is simulated in the test topology, then set the <i>Remote IP Address</i> to the N3 IP address of the UPF.

Notes:

- Paging objective should be configured with **Stateless UDP** as User Plane.
- Enter IDLE procedure is executed for each UE after Delay(s) once DN responds to instrumentation packet sent inband by the UE. See also *Global Settings > Advanced Settings > Traffic Settings > [Traffic Control Port](#)*.
- Following Enter IDLE, Downlink User Plane traffic is suspended for *Suspend Traffic Interval (s)*.

Enter/Exit Idle

When you configure an **Enter/Exit Idle** secondary objective, each of the active subscribers configured for the primary objective attempts to transition between the CM-IDLE and CM-CONNECTED states.

NOTE

When UE is scheduled to Exit Idle but the UE state is not Idle anymore (for example Paging event occurred), the Exit Idle procedure cannot be performed, therefore the Service Request is going to be skipped and the statistics for Service Request Skipped (on NG-RAN) will be incremented accordingly.

The following table describes the objective parameters.

Parameter	Description
<i>Enter Exit Idle:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated to transition UEs between the CM-IDLE state to the CM-CONNECTED states, measured in state transitions per second.
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	The number of seconds to wait between each successive state transition.

Create/Delete QoS Flows

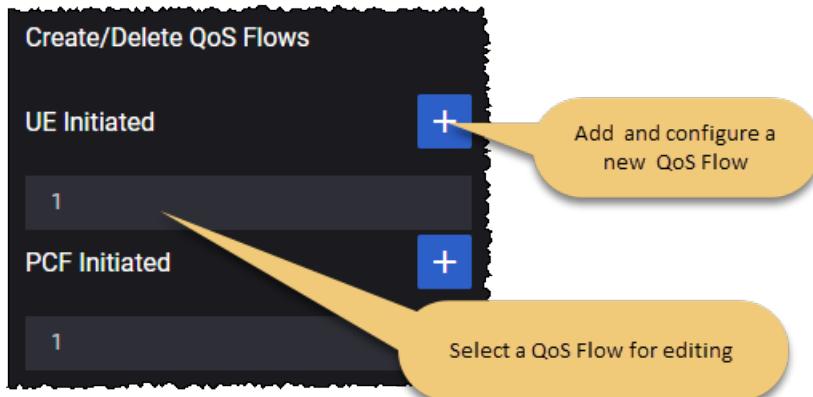
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured *Interval* expires.

QoS flow options

There are two options for creating QoS flows:

- UE initiated - the QoS flows are initiated by the UE
- PCF Initiated - the QoS flows are network initiated

The QoS Flow panel contains the configuration settings for an individual QoS Flow (UE initiated or PCF initiated).



Objective parameters

The following table describes the objective parameters (for both UE initiated QoS flows and PCF initiated QoS flows).

Parameter	Description
<i>Create/Delete QoS Flows:</i>	
	Select the Add Objective button to add an instance of this objective.
<i>Objective:</i>	
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameter requires a large number of UEs configured in the test in order to achieve the desired rate.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max	The maximum number of procedures that may be outstanding while new

Parameter	Description
Outstanding	procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	Interval between the triggering of creation and deletion of the QoS flow, in seconds.
DNN	Select the DNN value for the drop-down list. For example: dnn.keysight.com.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

Support for Network Initiated QoS Flow modification

The Create/Delete QoS Flows secondary objective also provides support for Network Initiated QoS Flow modification of existing QoS flows on the N1/N2 interfaces. This support is available when all topology nodes except for **RAN** are selected as DUTs.

By triggering the Network Initiated PDU Session Modification procedure, the network can modify the following parameters of the existing QoS flows, both default and dedicated:

- ARP
- QoS flow descriptions parameters (MBR, GBR)
- Session AMBR
- QoS rules – all supported filters

Notes:

- In order to modify the default QoS flow, it needs to be configured on the DNN tab. The QoS Flows and DNNs are configured in the Global Settings.
- None of the parameters changed by the network initiated QoS flow modification will be enforced.
- The NG-RAN node supports handling the QoS flow modification procedure only for one PDU session per procedure (Create QoS Flow, Modify QoS Flow, Release QoS Flow).
- For UE Initiated dedicated QoS Flows, the interval between the creation and deletion of the QoS flow should be large enough to support the successful finalization for the modification of the existing QoS flow. (*Interval* is one of the Objective settings.)

Create/Delete PDU Sessions

When you configure a **Create/Delete PDU Sessions** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements specified by the objective configuration. The PDU sessions will be created following a configured *Delay* value, and then deleted when the configured *Interval* expires.

The following table describes the objective parameters.

Parameter	Description
<i>Create/Delete PDU Sessions:</i>	
	Select the Add Objective button to add an instance of this objective.
<i>Objective:</i>	
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	<p>The rate at which procedures are initiated, measured in procedures initiated per second.</p> <p>Using higher values for this parameter requires a large number of UEs configured in the test in order to achieve the desired rate.</p>
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	The interval between the triggering of creation and deletion of the PDU Session, in seconds.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p>

Parameter	Description
	You configure DNNs for the selected UE in the DNNs Config Range settings. The list of available DNNs include those that have not been activated for the primary objective.

SMS

This objective will perform the procedure of sending SMS messages.

The following table describes the objective parameters.

Parameter	Description
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameters requires a large number of UEs configured in the test in order to achieve the desired rate.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Destination MSISDN	The MSISDN of the destination UE for the sent SMS.
Destination MSISDN Increment	The increment for the destination MSISDN.

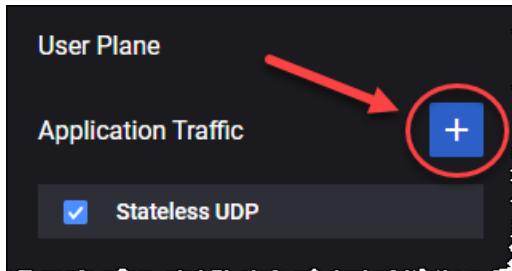
NOTE

No support for MT only SMS (Cu Isolation initiated SMS).

User Plane Objectives

The User Plane Objectives focus on the rate and volume of user plane traffic that the simulated UEs are sending to the 5G network. You define separate User Plane objectives for each UE range.

Cu Isolation provides multiple traffic application that can be added by selecting the **Add Objective** button.



NOTE

Based on your test requirements, the configuration of the User Plane Objectives may involve settings for the traffic generators on the UE and also on the DN. For the DN User Plane settings, refer to [DN User Plane](#).

The following table describes the Application Traffic generation parameters.

Parameter	Description
	Select this button to add a new application traffic objective. The objective can be: <ul style="list-style-type: none">• Stateless UDP• Data• Voice• Video OTT• DNS Client• Predefined Applications• ICMP Client• Capture Replay• Synthetic• UDG• Attacks• REST API Client
	Select this button to remove the application traffic objective from your test configuration.
Attacks	For the settings required to configure the Attacks traffic objective, refer to Attacks .
Stateless UDP	For the settings required to configure the Stateless UDP traffic objective, refer to

Parameter	Description
	Stateless UDP Traffic.
Data	For the settings required to configure the Data traffic objective, refer to Data Traffic.
Voice	For the settings required to configure the Voice traffic objective, refer to Voice Traffic.
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to Ott Traffic.
DNS Client	For the settings required to configure the DNS Client objective, refer to DNS Client Traffic.
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to Predefined Applications Traffic.
ICMP Client	For the settings required to configure the ICMP Client objective, refer to ICMP Client.
Capture Replay	For the settings required to configure the Capture Replay objective, refer to Capture Replay.
Synthetic	For the settings required to configure the Synthetic objective, refer to Synthetic.
UDG	For the settings required to configure the UDG objective, refer to UDG.
REST API Client	For the settings required to configure the UDG objective, refer to REST API Client.

Stateless UDP Traffic

The **Stateless UDP** objective generates IP packets that encapsulate dummy 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 .
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Flow Type	This field is set to uplink and cannot be modified since on the UE you can only configure the uplink flow.
Throughput Tx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change.

Parameter	Description
Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Limit Maximum Packet Rate per UE	If enabled, it will limit the Maximum Packet Rate per UE.
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
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.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For</p>

Parameter	Description
	example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.

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 .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Objective Type	By default, this parameter is set to Throughput . The other options are: Concurrent Connections and Connections Rate .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	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

Parameter	Description
	throughput.
Transmit buffer size (bytes)	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).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	Select the toggle button to enable this option.
<i>UDP Settings</i>	
Receive Buffer Size (bytes)	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.
Transmit Buffer Size (bytes)	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).
<i>TLS Settings</i>	See TLS Settings table for more details.
<i>Application Traffic Flows</i>	<p><i>Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.</i></p> <ul style="list-style-type: none"> • To select an existing traffic flow definition, click its name to open the

Parameter	Description
	<p><i>Flow panel where you can view and modify the flow settings.</i></p> <ul style="list-style-type: none"> • To add another traffic flow, click the Add Flow button. Cu Isolation will open the Flow panel where you will select the flow type and configure the flow settings. <p>Refer to Flow for a description of the configuration settings for these traffic flows.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

TLS Settings

Parameter	Description
TLSv1.2	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.2 is selected.</p>
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>IMPORTANT Session reuse method is available only if TLSv1.2 is selected.</p>
Session reuse count	<p>Specify how many simultaneous connections can share the same Session ID or Ticket.</p> <p>IMPORTANT Session reuse method is available only if TLSv1.2 is selected.</p>
TLSv1.3	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Middlebox compatibility	<p>Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>

Parameter	Description
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> If Optimize Throughput (per UE) option is enabled: TCP, TLS, QUIC or UDP. If Optimize Throughput (per UE) option is disabled: TCP, TLS or UDP.
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get, HTTP Put, HTTP Post and FTP. For TLS transport protocol: HTTPS Get, HTTPS Put and HTTPS Post. For QUIC transport protocol: HTTP3 Get, HTTP3 Put and HTTP3 Post. For UDP transport protocol: UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket) <p>NOTE UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receives the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds.</p>
Port	The 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 FTP server. <p>NOTE Setting the page size on UE side will only influence PUT objectives, like HTTP PUT, HTTPS PUT and FTP PUT. To set the page size for GET objectives, the change must be operated on DN side.</p>
Client Tx	This parameter is available only when the flow type is set to UDP Bidirectional.

Parameter	Description
Count	Refer to UDP Bidirectional for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
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.
Max Transactions per Connection	Set the value for this parameter.
DNN	Select the DNN for this flow. The DNNs are configured in the UE Range settings (DNNs Config).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

From this section you can add custom parameters or custom header fields by selecting the required pane:

- **Custom Parameters** or,
- **Custom Headers**

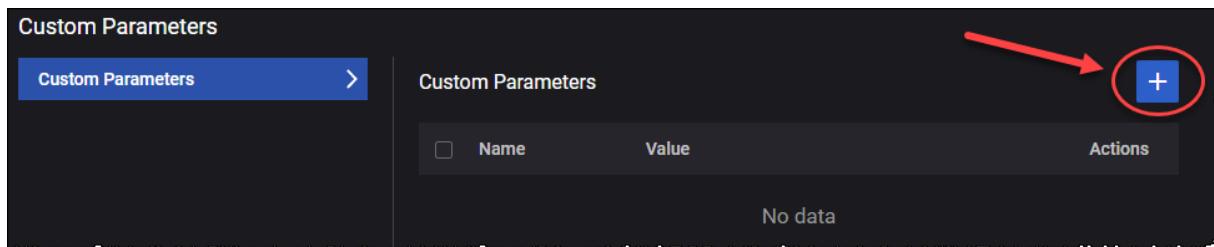
You can add custom parameters as follows:

1. Select the **Open Custom Parameters** button.



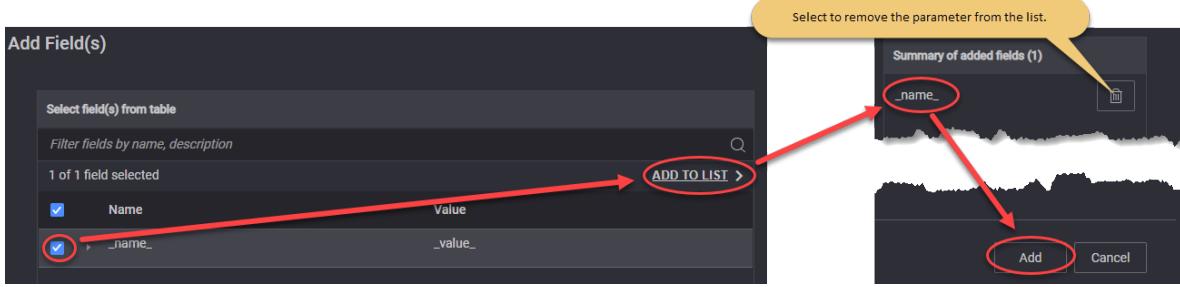
The Custom Parameters panel opens.

2. Select the **Add** button. The Add Field(s) opens.



3. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



To add custom header fields, select the **Custom Headers** pane and follow the steps presented above for custom parameters.

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 .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
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 .
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by Cu Isolation 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 • UDP - User Datagram Protocol

Parameter	Description
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Registration Refresh Time	Select the type of registration refresh time: <ul style="list-style-type: none"> Negotiated - Registration refresh will be sent after 50% of expiration time received in the <i>200 OK</i> response. Custom - it allows you to set your own interval.
Custom Registration Refresh Interval (s)	<p>IMPORTANT This parameter becomes available only the Registration Refresh Time is set to Custom.</p> <p>Set the registration refresh interval, in seconds.</p>
Number of Loops after Registration to Send De-Registration	A value of 1 means De-registration will have to occur on each loop with successful registration.
<i>Advanced SIP Settings</i>	<i>For more details about these settings, refer to Advanced SIP Settings.</i>
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by Cu Isolation or overwrite it with your own value.
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.
RTP Session Duration (ms)	Set the value for the session duration.
<i>Audio settings:</i>	<i>For the configuration of audio settings, refer to Audio Settings.</i>
<i>Video Settings:</i>	<i>For the configuration of video settings, refer to Video Settings.</i>
<i>MSRP Settings:</i>	<i>For the configuration of MSRP settings, refer to MSRP Settings.</i>
<i>MCTTP Settings</i>	<i>For the configuration of MSRP settings, refer to MSRP Settings.</i>
<i>Advanced Media Settings:</i>	
<i>Custom SDP</i>	<i>Select this panel to open the custom SDP settings.</i>
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list:

Parameter	Description
	<ul style="list-style-type: none"> • None • EVS/AMR IPv4 • NB Codecs IPv6 • AMR-WB IPv6 • Multimedia IPv4
<i>QoE Settings</i>	Select this panel to open the audio QoE settings.
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

Dial Plan

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

Parameter	Description
DNN	Select the DNN from the drop-down list.
Destination IP	The destination IP address.
Destination IP Increment	The value by which the destination IP is incremented.
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
MCC	<p>Set the mobile country code.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
MNC	<p>Set the mobile network code.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>

Parameter	Description
MSIN	The MSIN value that will be assigned to the first simulated UE in the range.
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 Port	The destination port number.

Audio Settings

The parameters required for audio settings are presented in the table below.

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for audio from the drop-down list.
<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	Select the audio codec from the drop-down list. The available options are: <ul style="list-style-type: none"> • AMR - 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-WB - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data

Parameter	Description
	<p>compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP.</p> <ul style="list-style-type: none"> • EVS - 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 <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 8 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 9 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	The following options are available: <ul style="list-style-type: none"> Full header - 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 Settings

The parameters required for audio settings are presented in the table below.

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Voice	Select the QoS Flows ID(s) from the drop-down list.
Video Codecs	<i>This section is available only when Enable video is selected</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	Select the audio codec from the drop-down list. The available options are: H264 or H265 .
FPS	Set the FPS value.
Payload Type	Set the payload type value.

Parameter	Description
Average Bitrate (kbps)	Set the average bit rate value.

MSRP Settings

The parameters required for MSRP settings are presented in the table below.

Parameter	Description
Enable MSRP	Select to enable this option.
QoS Flow ID for MSRP	Select the QoS Flows ID(s) from the drop-down list.
MSRP Port	Provide the MSRP port.
MSRP Local domain	Provide the MSRP local domain.

MCPTT Settings

The parameters required for Mission Critical Push to Talk (MCPTT) settings are presented in the table below.

Parameter	Description
Enable MCPTT	Select to enable this option.
QoS Flow ID for MCPTT	Select the QoS Flows ID(s) from the drop-down list.
MCPTT Message Format	The MCPTT message format defined according to TS 24.380 standard.
MCPTT Group	A defined set of MCPTT Users identified independently of transport or network type.
MCPTT Group Size	The number of participants per MCPTT group call.
Use CRLF in flow csv	If enabled, it will use the CRLF line terminator in the generated CSV of the configured MCPTT flow. If disabled, it will use LF.

Advanced SIP Settings

The following settings are available under the Advanced SIP Settings section:

- [SIP Custom Headers](#)
- [SIP Authentication](#)
- [Custom Parameters](#)
- [SIP 3GPP IPSEC](#)

SIP Custom Headers

From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

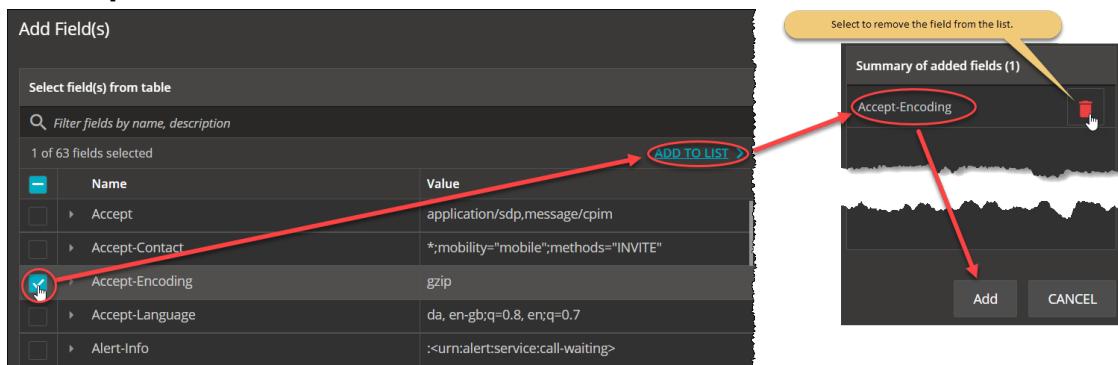
NOTE

The message can be deleted by selecting the corresponding **Delete** for each message. Also, you can use the **Edit** button for bulk selection and, then, delete the message in one action.

For each message, you can:

- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
 - Select the **Add** button. The Add Field(s) opens.
 - From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



The following custom header are available:

Parameter	Description	Value
Accept	IETF RFC 3261	application/sdp,message/cpim
Accept-Contact	IETF RFC 3841	*;mobility="mobile";methods="INVITE"
Accept-Encoding	IETF RFC 3261	gzip
Accept-Language	IETF RFC 3261	da, en-gb;q=0.8, en;q=0.7
Alert-	IETF	<urn:alert:service:call-waiting>

Parameter	Description	Value
Info	RFC 3261	
Allow	IETF RFC 3261	INVITE, ACK, UPDATE, PRACK, CANCEL, PUBLISH, MESSAGE, OPTIONS, SUBSCRIBE, NOTIFY
Allow-Events	IETF RFC 6665	conference
Authentication-Info	IETF RFC 3261, IETF RFC 3310	nexnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	<http://www.example.com/alice/photo.jpg> ;purpose=icon
Content-Disposition	IETF RFC 3261	session
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:00 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>

Parameter	Description	Value
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC 3261	3600
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC 4028	60
Organization	IETF RFC	Keysight

Parameter	Description	Value
	3261	
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC 3327	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>
P-Called-Party-ID	IETF RFC 7315	sip:user1-business@example.com
P-Charging-Function-Addresses	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Charging-Vector	IETF RFC 7315	icid-value=1234bc9876e;icid-generated-at=192.0.6.8;orig- ioi=home1.net
P-Early-Media	IETF RFC 5009	supported
Permission-Missing	IETF RFC 5360	userC@example.com
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel

Parameter	Description	Value
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=FALSE,algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>,<sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org?Replaces=425928%40bobster.example.com.3%3Btag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path

Parameter	Description	Value
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition

Parameter	Description	Value
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

SIP Authentication

The parameters required for SIP authentication are presented in the table below.

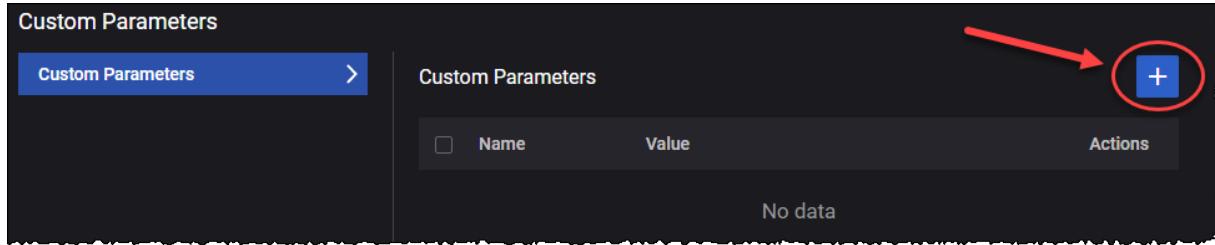
Parameter	Description
Username	Provide the username.
Password	Provide the password.
Authentication Type	Select the authentication type: <ul style="list-style-type: none"> • Digest MD5 • AKAv1 • AKAv2 • ProxyDefined
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by Cu Isolation, or enter of a K value of your own choosing.
K Increment	The number used to increment the K value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same K value.
Configure OP or OPc	Select the operator-specific authentication value.
Op	The Auth OP value specifies the operator-specific authentication value to use

Parameter	Description
	for the UEs in this range. It is a string with a maximum length of 34 characters. It remains fix for all Subscriber/SIM of an operator. You can accept the value generated by Cu Isolation, or enter of an OP value of your own choosing.
Opc	The OPC value is derived from the subscriber key K and the operator dependent value OP. You can accept the value generated by Cu Isolation, or enter of an OP value of your own choosing.
Opc Increment	The number used to increment the OPC value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same OPC value.

Custom Parameters

You can add custom parameters as follows:

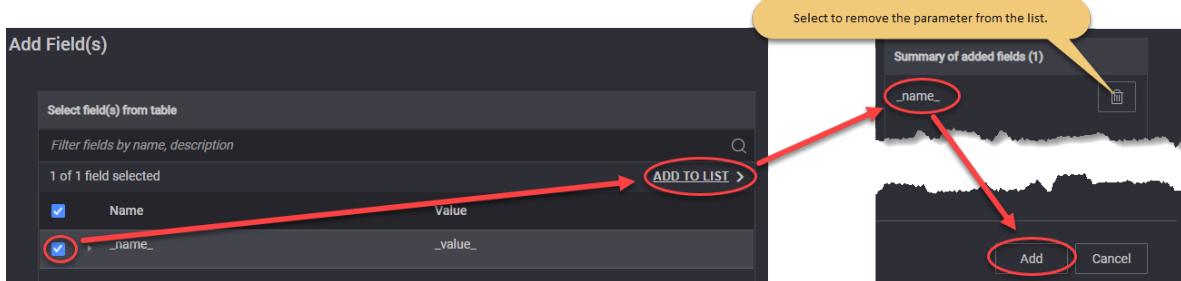
1. The Custom Parameters panel, select the **Add** button.



The Add Field(s) opens.

2. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



The following custom parameters are available:

Parameter	Description	Value
DelayBefore SIPInvite	Delay in milliseconds before sending SIP INVITE.	1000
DealyBeforeRTP	Delay in milliseconds before RTP session start.	0

Parameter	Description	Value
DelayAfterRTP	Delay in miliseconds after RTP session end.	0
DeregisterLoop	Set the number of calls/loops before a SIP deregistration will be performed. Any SIP deregistration will be followed by a new SIP registration.	0
DelayBefore180	Delay in miliseconds before 180 Ringing message will be sent.	0
DelayBefore200INVITE	Delay in miliseconds before 200 OK message for INVITE will be sent.	0
debugIPSEC	Activate IPSEC debug. Please use debug only for a reduced number of simulated UEs.	0
timeoutSIP	Global timeout in miliseconds for any SIP message. Default is set to standard 32000ms. Use this parameter to modify the default value.	32000
MaxActiveLimit	Set maximum allowed concurrent TCP connections per CPU Core. Default it is set to 8000. Please use this parameter to modify the default value.	8000

SIP 3GPP IPSEC

The parameters required for SIP 3GPP IPSEC are presented in the table below.

Parameter	Description
Port-C	Set the value for this parameter.
Port-S	Set the value for this parameter.
Authentication Algorithm	Select the authentication algorithm: <ul style="list-style-type: none"> • hmac-sha-1-96 • aes-gmac • null
Encryption Algorithm	Select the encryption algorithm: <ul style="list-style-type: none"> • aes-gcm • aes-cbc • null

Video OTT Traffic

The following table describes the Video 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 .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Objective Type	Select the value from the drop-down list: Simulated Users or Throughput .
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.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).

Parameter	Description
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	Select the toggle button to enable this option.
<i>UDP Settings</i>	
Receive Buffer Size (bytes)	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.
Transmit Buffer Size (bytes)	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).
<i>TLS Settings</i>	See TLS Settings table for more details.
Advanced OTT	<p><i>Each Application Traffic entry requires at least one Ott traffic flow definition, and can support multiple such definitions.</i></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. Cu Isolation will open the Flow panel where you will select the flow type and configure the flow settings. <p>Select the Open Advanced OTT button to enable and configure Advanced OTT Settings.</p>

TLS Settings

Parameter	Description
<i>TLSv1.2</i>	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.2 is selected.</p>
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>IMPORTANT Session reuse method is available only if TLSv1.2 is selected.</p>
Session reuse count	<p>Specify how many simultaneous connections can share the same Session ID or Ticket.</p> <p>IMPORTANT Session reuse method is available only if TLSv1.2 is selected.</p>
<i>TLSv1.3</i>	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Middlebox compatibility	<p>Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.

Advanced OTT Settings

The parameters required to configure the OTT advanced settings are presented in the table below.

Parameter	Description
<i>Flow:</i>	

Parameter	Description
	Select this button to remove this flow from your test configuration.
Type	Select the Ott traffic type from the drop-down list. Available options: <ul style="list-style-type: none"> • DASH • HLS
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
URL	Select the URL from the drop-down list populated with the defined on the server.
Play Until End	If this check box is selected, the Play Duration field is disabled and the original playtime is used.
Play Duration (sec)	This field is available only if the Play Until End check box is not selected. It allows you to set a custom playtime.
Transport	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/QUIC
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero).
Percentage	The percentage of Test Objective to execute this flow.
<i>Quality Control</i>	<i>These settings are presented in the Quality Control pane.</i>
<i>Advanced Client settings</i>	<i>These settings are presented in the Advanced Client Settings pane.</i>

Quality Control

The parameters required for Quality Control settings are presented in the table below.

Parameter	Description
<i>Jitter Buffer:</i>	
Initial Delay (s)	Set the number of seconds to wait before playback. The default value is 20.
Maximum Size (s)	Set the number of seconds to be buffered on the client side. The default value is 20.

Parameter	Description
MOS P.1203	Select an option from the drop-down list: Disabled or Mode 0 .
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> • Adaptive Bit Rate • Quality Predefined Levels • Lowest Quality • Highest Quality
Number of segments	This field is available and editable only when the Quality Control Mode is set to Adaptive Bit Rate .
<i>Play Profiles: The following settings are available and editable only when the Quality Control Mode is set to Quality Predefined Levels.</i>	
	Select this button to add a predefined play profile to your test configuration.
<i>Quality Shift</i>	
	Select this button to remove this play profile from your test configuration.
Shift Type	Select the shift type from the drop-down list. Available options <ul style="list-style-type: none"> • Stay at Current Bitrate • Change to the Lowest Bitrate • Change to the Lowest Bitrate • Change to the Lower Bitrate • Change to the Higher Bitrate
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to Change to Higher Bitrate or Change to Lower Bitrate .
Play Until End	If this check box is selected, the Play duration field is disabled and the original playtime is used.
Pay duration(sec)	This field is available only if the Play Until End check box is not selected. It allows you to set a custom playtime.

Advanced Client Settings

The parameters required for Advanced Client settings are presented in the table below.

Parameter	Description
DNN ID	Select the DNN from the drop-down list.

Parameter	Description
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
Timeshift for Live	Set a value for this field. 0 means no timeshift.
Enable DNS Query Per Connection	Select the check box to process only one DNS query per TCP connection.
Custom Parameters	For more details, refer to Custom parameters and headers .
Custom Headers	For more details, refer to Custom parameters and headers .

Custom Parameters and Headers

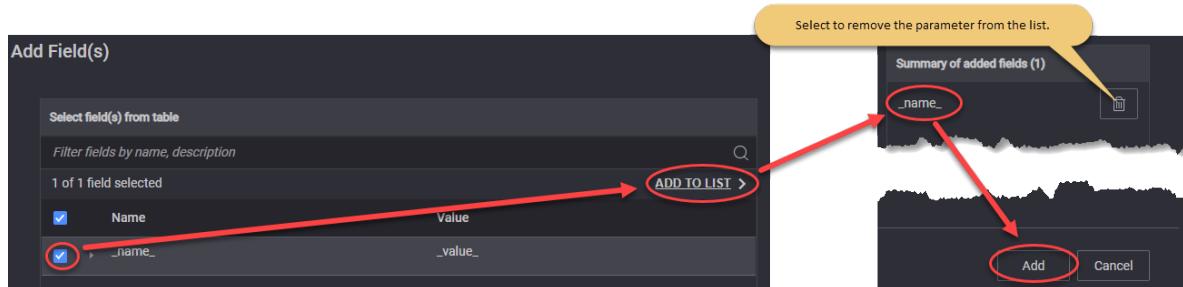
From this section you can add custom parameters or custom header fields:

- **Custom Parameters** or,
- **Custom Headers**

You can add custom parameters as follows:

1. Select the **Custom Parameters** pane.
The Custom Parameters panel opens.
2. Select the **Add** button. The Add Field(s) opens.
3. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



To add custom header fields, select the **Custom Headers** pane and follow the steps presented above for custom parameters.

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 .
Label	Set the label name. You can accept the default value or overwrite it with your own value.

Parameter	Description
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.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Application Traffic Flows	<p><i>Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.</i></p> <ul style="list-style-type: none"> <i>To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</i> <i>To add another traffic flow, click the Add Flow button. Cu Isolation will open the Flow panel where you will select the flow type and configure the flow settings.</i> <p><i>Refer to Flow for a description of the configuration settings for these traffic flows.</i></p> <p><i>Also, you can add custom parameters, based on your test configuration requirements.</i></p>

Flow

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

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	Select the query type from the drop-down list. The available options are:

Parameter	Description
	<ul style="list-style-type: none"> • A • AAAA
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.
DNN	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Config).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

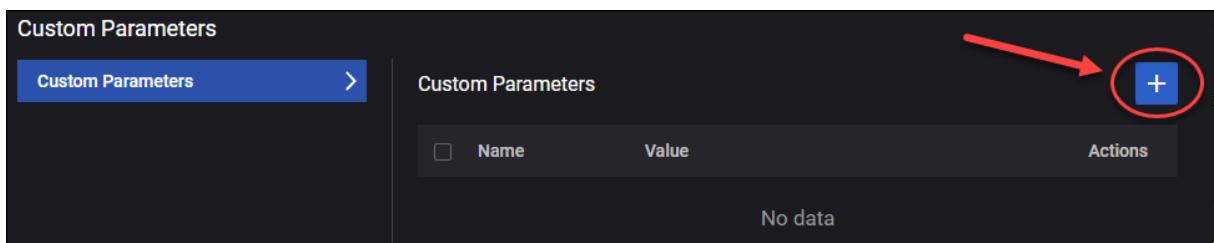
You can add custom parameters as follows:

1. Select the **Open Custom Parameters** button.



The Custom Parameters panel opens.

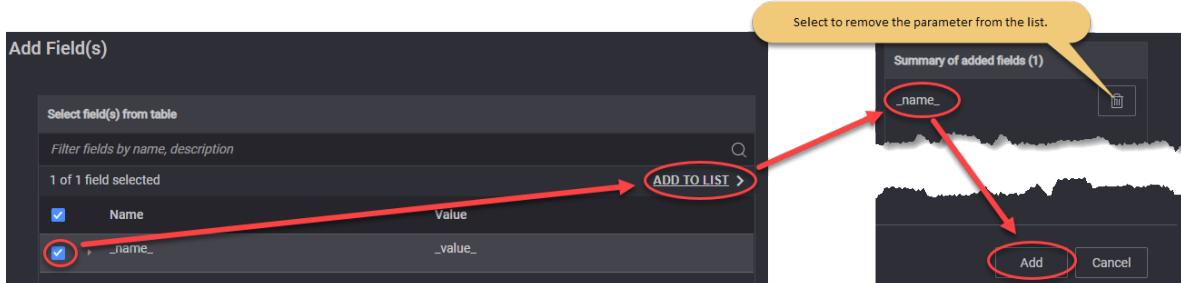
2. Select the **Add** button.



The Add Field(s) opens.

3. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



ICMP Client

The following table describes the ICMP Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to ICMP Client .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Traffic Flow	Refer to Traffic Flow for a description of the configuration settings for these traffic flows.

Traffic Flow

The **Traffic Flow** parameters are described in the following table.

Parameter	Description
Destination Hostname	Set the destination hostname.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.
Interval (ms)	Set the interval value.
Timeout (ms)	Set the timeout value.
DNN	Select the DNN for this flow. The DNNs are configured in the UE Range Settings.

Capture Replay

This page describes the settings required by the capture replay functionality. Ethernet-based packet captures (.pcap files) can be filtered and resulting packets can be replayed on top of GTPu tunnels. Packets can be replayed as Ethernet frames over Ethernet PDU sessions or as IPv4 or IPv6 frames over IP-based PDU sessions. The capture replay feature can also be used with SGi client and SGi server (DN) to replay IP and Ethernet frames without any additional encapsulation.

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Capture Replay .

Parameter	Description
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Capture File	It allows you to upload a capture file, using the Upload button. To remove the file, select the Clear button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to 0 for no limit. The default value is 1 .
Maximum Packet Rate (pps)	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Limit Maximum Packet Rate per UE	If enabled, it will limit the Maximum Packet Rate per UE.
Rx Timeout (ms)	Time the responder waits for packets, after the delay observed in the packet capture. The default value is 1000 miliseconds.
Delayed Tx	Prevent the packets from being sent faster than they appear to be sent in the capture file, trying to maintain the packet delays. The default value is true (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is true (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field).

Parameter	Description
	This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.

The following table describes the **Filter** object parameters.

Parameter	Description
<i>Filter</i>	
	Select this button to add a new filter to your test configuration.
	Select this button to remove the additional route from your test configuration.
Role	Select the role from the drop-down list. Available options: Initiator and Responder . Default value: Initiator .
Filter Expression	This field cannot be empty. It selects the packets to be replayed from uploaded capture. The filter string should be in pcap-filter format, as described at https://www.tcpdump.org/manpages/pcap-filter.7.html .
Remove Encapsulation	Remove GTPu encapsulation from packets, if present, before trying to match the filter expression and when replaying the packets. The default value is false (option disabled).
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to Initiator . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Synthetic .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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 that the computed RTO timer value can be set to.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).

Parameter	Description
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).

The following table describes the **Traffic Flow** parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP .
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Throughput Tx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (bytes)	IMPORTANT This field is available only when Transport Protocol is TCP. The number of bytes the client sends in a burst.
Client Burst Size (packets)	IMPORTANT This field is available only when Transport Protocol is UDP. The number of packets the client sends in a burst.

Parameter	Description
Client Packet Size (bytes)	IMPORTANT This field is available only when Transport Protocol is UDP. The packet size in bytes.
Client Timeout (ms)	IMPORTANT This field is available only when Transport Protocol is UDP. Set the timeout value.
Throughput Tx (kbps)	IMPORTANT This field is available only when Transport Protocol is UDP. This value is computed based on the parameters in the test and will be recalculated if one of these parameters change. A corresponding server is required to achieve the displayed value.
Server Burst Interval (ms)	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	IMPORTANT This field is available only when Transport Protocol is UDP. The number of packets the server sends in a burst.
Server Packet Size (bytes)	The packet size in bytes.
Server Timeout (ms)	IMPORTANT This field is available only when Transport Protocol is UDP. Set the timeout value.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

UDG

The following table describes the **UDG** parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to UDG .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .

Parameter	Description
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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 that the computed RTO timer value can be set to.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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,

Parameter	Description
	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).

The following table describes the **Traffic Flow** parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP .
Out of Band Signaling	<p><i>Select this check-box to enable OOB signaling. More details about the required parameters here.</i></p> <p>IMPORTANT <i>To use the OOB feature, the OOB interface must be set in Agent Management window.</i></p>
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Source Port	The local port for client data connection.
Reconnect Timeout (ms)	The time interval after which the client attempts to reconnect after the connection was interrupted. 0 means that reconnect is disabled.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
UDG Traffic Parameters	<i>Select to enable and configure the UDG Traffic Parameters.</i>
Transaction	<i>Select to enable and configure the Transaction parameters.</i>
Status Query Interval	Timeout for keepalive packets on server. The server will wait for the <code>keepAliveInterval</code> value multiplied by <code>keepAliveExpiryCount</code> value.
Keepalive Interval	The time interval, in milliseconds, between UDG statistics requests (RESULT). A zero value means this feature is disabled.

Parameter	Description
Keepalive Expiry Count	The time to wait for UUDG to reconnect. A 0 value means the reconnect is disabled (in milliseconds).

The following table describes the **Out of Band Signaling** parameters.

Parameter	Description
Local Address	The local IP address.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Remote Address	The remote IP address.
Port	Set the used port.

The following table describes the **UDG Traffic Parameters**.

Parameter	Description
UDG Test Type	Select the test type from the drop-down list. Available options: Transmission, Ping-pong or Speed-Test . For each test type, the parameters are described below.
<i>Transmission</i>	
Throughput Tx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Interval Unit	The unit in which this burst interval is expressed.
Client Burst Size (packets)	The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Throughput Rx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change.

Parameter	Description
	A corresponding server is required to achieve the displayed value.
Server Burst Interval (ms)	The time interval at which the server sends packet bursts.
Server Burst Interval Unit	The unit in which this burst interval is expressed.
Server Burst Size (packets)	The number of packets the server sends in a burst.
Server Burst Interval Unit	Select the server burst interval unit. Available options: Millisecond or Microsecond .
Server Burst Size (bytes)	The packet size in bytes.
<i>Ping-pong</i>	
Ping Direction	Set the ping direction. Available options: Upstream or Downstream .
Ping Interval	Set the ping time interval.
Ping Interval Unit	Set the ping interval unit. Available options: Millisecond or Microsecond .
Pong Number	Set the value for the pong number.
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.
<i>Speed-Test</i>	
Traffic direction	Select the traffic direction for which this filter applies: Uplink or Downlink .
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.

The following table describes the **Transaction** parameters.

Parameter	Description
<i>Transaction</i>	Select the check-box to enable these settings.
Duration (ms)	Transactions duration, in millisecond.

Parameter	Description
Idle interval (ms)	Idle interval between transactions, in millisecond.
Resume Mode	Side which triggers transition between the UE idle and the UE connected state. Available options: User or Network .

Attacks

The **Attacks** objective simulates multiple type of attacks (more than 7000 of profile attacks available).

The following table describes the Attacks parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Attacks .
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Objective Type	This field is set to flow and cannot be modified.
Attacks per second	The rate of attacks initiated per second.
Iterations	If is set to 0 , it will be iterated on continuous loop during sustain time. If set to 1 , it will be executed only one time. IMPORTANT Values greater than 1 are not allowed.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before starting the Attacks objective traffic.
Configure Attack Profiles	<i>Press the button to open the Attacks settings page.</i>

Attack Profiles

IMPORTANT Fore this section to work properly, make sure you have installed the latest ATI security updates.

You can add more attack profiles as follows:

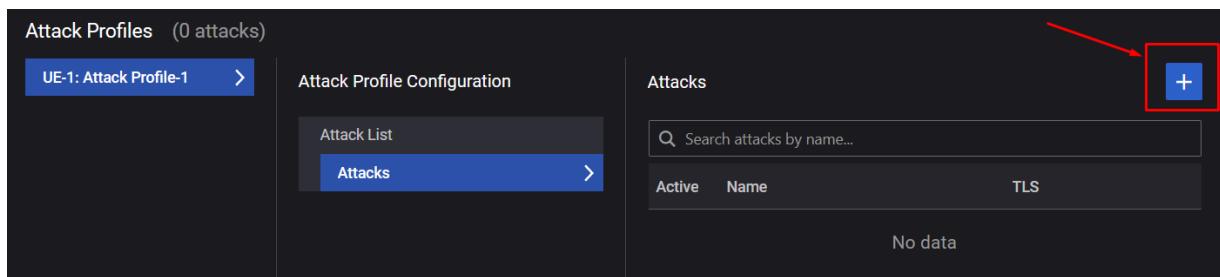
1. Select the **Open Configure Attack Profiles** button.

Configure Attack Profiles



2. The Attack Profiles panel opens. Select the existent attack profile to open the **Attack Profile Configuration** panel.

3. A list with all profile attacks is displayed. Click on an the **Attacks** to open the configurator, then select the **Add** button.



4. The **Add Attack(s)** dialog opens. Next you can select which attacks to be added to your profile:
- use the **Attack Library** tab to select and add ready-made attacks. See [Adding attacks from the Library](#)
 - use the **Customize Attack** tab to add modified sets of attacks according to your needs. See [Adding customized attacks](#)
5. Once you complete Step 4, the attacks will be added to your list. Allow a few seconds for the list to load. Further actions include:
- edit each attack - see [Editing attacks](#) for details.
 - add more attacks at any time, or **Edit** the list and (bulk) remove the attacks no longer required in the current profile.
6. For each **Attack Profile** added, The following section will become available and will require configuration:
- [TCP Settings](#)
 - [TLS Settings](#)
 - [HTTP Settings](#)

Adding attacks from the Library

In the **Attack Library** tab, you can do the following:

Panel	Description
Filter attack(s)	You can filter the attacks by category name or value.
Attacks category panel	Each category listed includes more sub-categories and the number of existing attacks per each. Select a category/sub-category check-box to see the attacks included in the main panel
Select attack(s) from the table panel	The middle panel will be populated with the results of your filtered search. More actions include: <ul style="list-style-type: none"> further filter the attacks to add the one you need. expand each attack to see a complete description and details about it. press the Add icon (+) at the end of the row to select the attack to your profile.

Panel	Description
Summary of added attack(s) panel	You can view and manage the list of selected attacks. Press the Delete icon (trash bin) if you want to remove any of the attacks.
Add button	Once you have finished the selection, press this button to complete your action. The attacks will be added to your profile.

Adding customized attacks

From the **Customize Attack** tab, you can:

Panel	Description
Select target application (optional) panel	Filter by the targeted application name to narrow down the results. TIP If you use this filter, it will automatically add specific strikes to the Insert Strike(s) panel.
Filter strikes panel	You can filter the attacks by category name or value. Each category listed includes more sub-categories and the number of existing attacks per each. Select a category/sub-category check-box to see the attacks included in the main panel

Panel	Description
Select strike(s) from the list	<p>This panel will be populated with the results of your filtered search (second panel search). More actions include:</p> <ul style="list-style-type: none"> • further filter the strikes to add the one you need. • expand each attack to see a complete description and details about it. • select the attacks you need
Insert strike(s) panel	<p>Depending on which of the previous options you have used, inserting strikes can be done in two ways:</p> <ul style="list-style-type: none"> • press the Add button (+) in the empty list to add the selected strikes (this is applicable when selecting from the category list in the second panel) • select an Add button under/above an application strike that is already added in the list to mark the place and the order of execution for the selected category strike. <p>TIP The category strikes will appear in the list with a dark red hallow.</p>
Add button	Once you have finished the selection, press this button to complete your action. The attacks will be added to your profile.

The screenshot shows the 'Add Attack(s)' dialog with four main sections:

- Select target application (optional):** Shows a list of applications including 'Alibaba' (selected), 'Amazon Chime', etc. A red arrow points from the 'Alibaba' entry to the 'Filter strikes' section.
- Filter strikes:** Shows filters for 'Date' (with '8 (1)' checked) and 'Other'. A red arrow points from the '8 (1)' checkbox to the 'Select strike(s) from list' section.
- Select strike(s) from list:** Shows a table with one strike: 'Strike Novell Groupwise Client Activ...' (Severity: High, Direction: s2c, Reference: CVE: 2012-0439). A red arrow points from this section to the 'Insert strike(s)' panel.
- Insert strike(s):** Shows a list of seven strikes: 1. Strike Novell Groupwise..., 2. Get Sign In Page, 3. Sign In, 4. Searching for product, 5. Buy product or contact seller, 6. Get Main Page, 7. Sign Out. The first strike is highlighted with a red box.

Editing attacks

Each attack added to the list can be edited or removed. To inspect and further edit an attack:

1. Note that the attack row shows several quick action icons and details:

Icon	Action Button	Description
	Activate button	Enable/disable the attack in this profile.
	TLS	Hover over this icon to see the TLS status for this attack. You can quickly view the TLS settings behind this status. For further details on this setting, see Application Advanced Settings > TLS Settings .
	Rename	Click this icon and change the name of the attack.
	Advance Settings	Press this button to open the Advance Settings page.
	Delete	Click to delete the attack from the list.
	Move	Drag up or down to change the item's position in the list.

2. To configure the setting, select an attack. The **Attack Settings** panel will open. Configure the parameters, or further edit the attack.

Parameter	Description
<i>Attack Settings</i>	
Destination Hostname	Destination hostname of the server.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
<i>Attacks Strikes and Actions</i>	
	Edits the strikes in the list. This will enable selecting and removing the strikes from the list.
	Add strikes and Actions button. This will open the Add strikes and Actions configuration dialog, where you can select and add more attacks to the selected attack, or assign actions.
	Connect strikes to server endpoint. This will open the Misc Browser Attacks - Connect Strikes to Server Endpoints page, where you can select and link the strikes that need to connect to a server.
Strikes and	When selecting a strike from this list, you can:

Parameter	Description
actions list	<ul style="list-style-type: none"> remove the strike from the list drag up or down to change the item order configure specific properties for the selected strike, in the Properties panel. Refer to Cu Isolation Application Actions appendix for further details.

REST API Client

The **REST API Client** objective simulates RESTful clients conforming to the design principles of the representational state transfer (REST) architectural style. Simulated clients are designed for one-arm testing, being fully interoperable with real RESTful Servers.

The following table describes the REST API Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to REST API Client .
Label	Set the label name. You can accept the value provided by Cu Isolation or overwrite it with your own value.
Objective Type	This field is set to Simulated Users and cannot be modified.
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP
REST API Flow	<p>The name of list of REST API Client sequential operations and transitions emulated by each REST API Client.</p> <p>The REST API Flow is initially loaded into LoadCore's Resource Library, and then added to the test as a Global Playlists. The list is defined in CSV format, following specific rules. Refer to <i>Keysight Open RAN Simulators, Cloud Edition 5.0 LoadCore User Guide</i> for further information.</p>
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before starting the Attacks objective traffic.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
Iterations	If is set to 0 , it will be iterated on continuous loop during sustain time. If set to 1 , it will be executed only one time. IMPORTANT Values greater than 1 are not allowed.
Max Transactions per Connection	The maximum amount of transactions an application can make on one connection.

Parameter	Description
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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).
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Selective Acknowledgments	Select the toggle button to enable this option.
<i>TLS Settings</i>	See TLS Settings table for more details.

Parameter	Description
Custom Parameters	For more details, refer to Custom parameters .

TLS Settings

Parameter	Description
TLSv1.2	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.2 is selected.</p>
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>IMPORTANT Session reuse method is available only if TLSv1.2 is selected.</p>
Session reuse count	<p>Specify how many simultaneous connections can share the same Session ID or Ticket.</p> <p>IMPORTANT Session reuse count is available only if TLSv1.2 is selected, and Session reuse method is set to Session Ticket or Session ID.</p>
TLSv1.3	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	<p>Select one or more ciphers from the drop-down list.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Middlebox compatibility	<p>Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.</p> <p>IMPORTANT This parameter becomes available only if TLSv1.3 is selected.</p>
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.

Custom Parameters

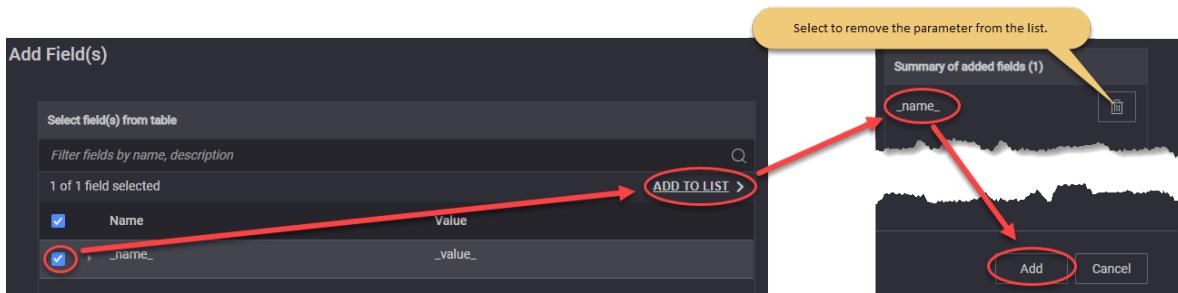
From this section you can add custom parameters fields:

- **Custom Parameters**

You can add custom parameters as follows:

1. Select the **Custom Parameters** pane.
The Custom Parameters panel opens.
2. Select the **Add** button. The Add Field(s) opens.
3. From the Add Field(s), select the fields you want to add and select **ADD TO LIST** to move them to the added fields section. To add the fields to your configuration select **Add**.

For example ...



Predefined Applications Traffic

The following table describes the Predefined Flows Traffic parameters.

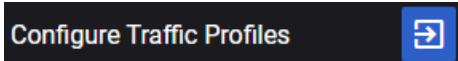
Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Simulated Users • Throughput • Connections Per Second
Throughput (kbps)	IMPORTANT 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.
Connections Per Seconds	IMPORTANT This parameter is available only when Objective Type is set to Connections Per Second . Set the number of connections.

Parameter	Description
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
<i>Configure Traffic Profiles</i>	<p><i>Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions.</i></p> <p><i>Refer to Traffic Profile for a description of the configuration settings for these traffic profiles.</i></p>

Traffic Profile

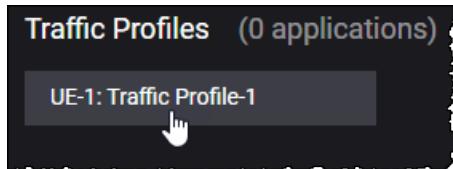
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

1. Select the **Configure Traffic Profiles** button.



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

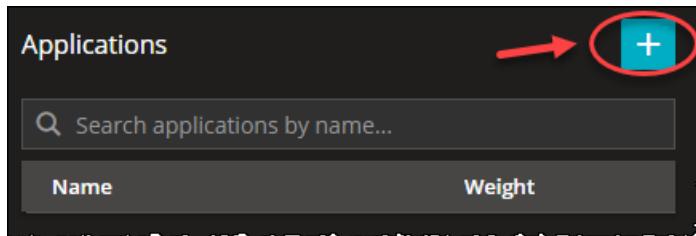
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

- [Applications](#)
- [TCP Settings](#)
- [TLS Settings](#)
- [HTTP Settings](#)
- [RTP Settings](#)

Applications

You can add or remove predefined applications from the Applications tab under the Traffic Profile Configuration section, as follows:

1. Select the **Add Application** button.



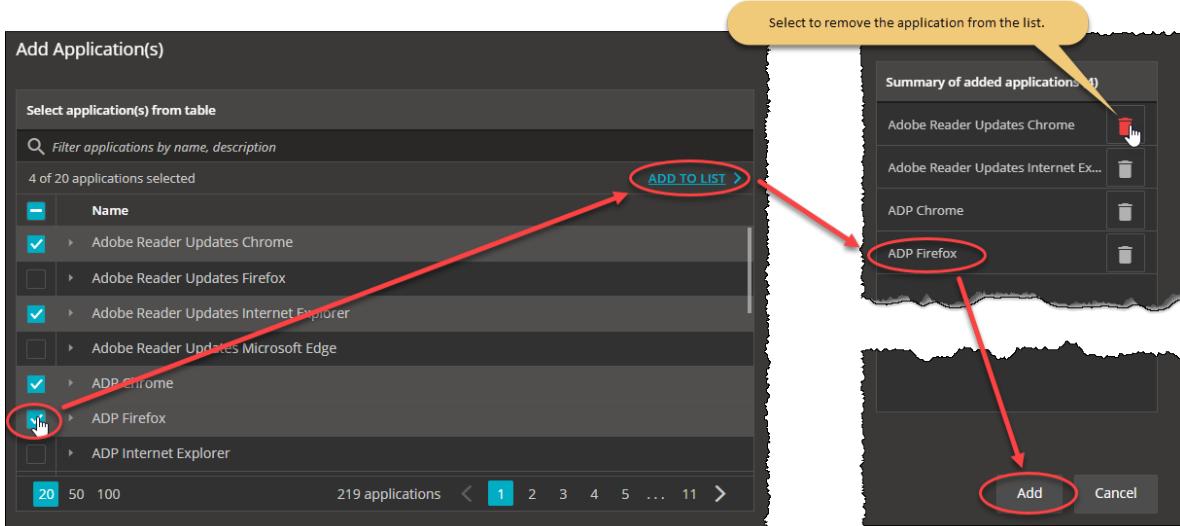
The Add Application(s) window opens.

2. From the Add Application(s), select the applications you want to add and select **ADD TO LIST** to move them to the added applications section. To add the applications to your configuration select **Add**.

NOTE

For the complete list of predefined applications, refer to [Predefined Applications](#).

For example ...



The applications are added to your configuration under the Applications section.

For example ...

Name	Weight	
Adobe Reader Updates Chrome 1	1	
Adobe Reader Updates Internet Exp...	1	
ADP Chrome 3	1	
ADP Firefox 4	1	

3. If needed, you can select the **Edit** button to enable the bulk selection of the available applications in order to remove them from the list.

For each application added, the following elements are available in the Applications table:

Field	Description
Name	The application name.
Weight	Set the application weight using the adjustment button. If the primary objective of a Traffic Profile is set to Throughput , the selected weight distribution time depends on the types and number of applications added to the application list.
Action Buttons	<ul style="list-style-type: none"> • Rename - Select to rename the application. • Advanced Settings - for more information, refer to Advanced Settings. • Delete - Select to delete the application.

When an application is selected from the Application table, the Application Settings and Application Actions sections are displayed.

For example ...

The screenshot shows the 'Applications' management interface. On the left, there is a list of predefined applications with columns for Name and Weight. One application, 'Adobe Reader Updates Chrome 1', is selected and highlighted with a cursor. On the right, two sections are displayed: 'Application Settings' and 'Application Actions'. The 'Application Settings' section contains fields for Destination Hostname, DNN ID, and QoS Flow ID. The 'Application Actions' section lists actions such as 'Check For Updates' and 'Download Updates'.

#	Name
1.	Check For Updates Client -> Server acroipm2.adobe.com
2.	Download Updates Client -> Server ardownload.adobe.com

Application Settings

Under the Application Settings section, the following fields are displayed:

NOTE These fields under the Application Settings section are common to all predefined applications.

Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

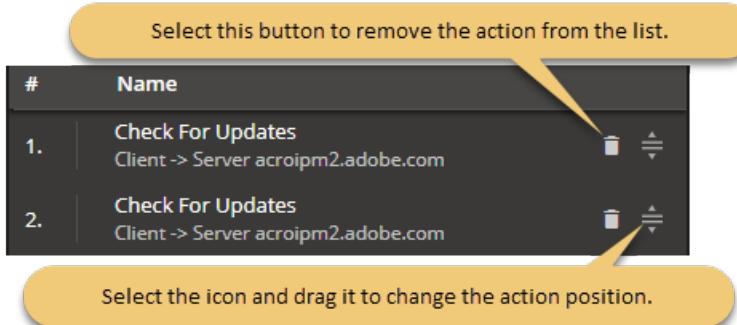
Application Actions

The Application Actions section lists the actions and action parameters available in Cu Isolation for each predefined application. For the complete list of actions and parameters, refer to Application Actions section in *ORAN SIM CE CoreSIM User Guide*.

Under the Application Actions section, you can edit or add new actions for each application:

1. Use the icons available for each icon in order to remove it or to change its position in actions list.

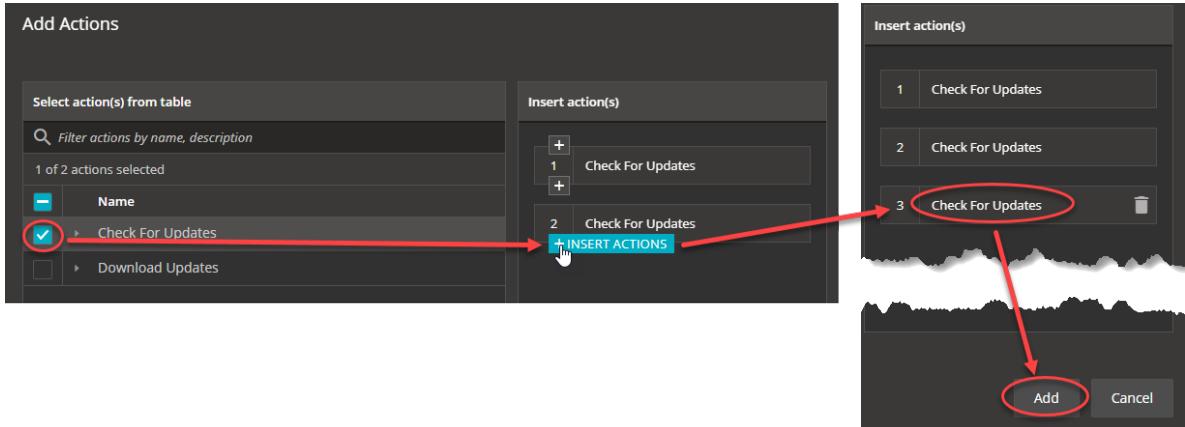
For example ...



2. Select the **Add Actions** button to add new actions to the application. The Add Action(s) window opens.

Select an action from the list and then use the **Insert Actions** button to add the action in the desired position on the Insert Action(s) table. Select **Add**.

For example ...



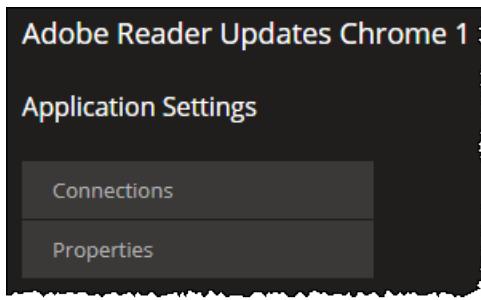
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

Application Advanced Settings

For each predefined application, the Application Settings menu is displayed when the Advanced Settings button is selected. This menu contains two main sections:

- **Connections**
- **Properties**

For example ...



Under the **Connections** section, the Connections table is displayed. When a connection is selected, the Connections Properties fields are displayed, as follows:

Field	Description
Name	The application name.
Client Endpoint	The client endpoint.
Server Endpoint	The server endpoint.
Hostname	The hostname name.
Destination Port	The TCP source port that the client endpoint is initiating connections from.
Server Port	The TCP port that the server endpoint is accepting connections on.
Encryption disabled	Select the check box to enable it this option.

Under the **Properties** section, the application settings Properties fields are displayed, as follows:

Field	Description
Name	The application name.
Iterations	Set the value for the number of iterations.
Max Transactions	The maximum amount of transactions an application can make.
Client HTTP profile	Select the client HTTP profile from the drop-down list. The available options are: <ul style="list-style-type: none"> • Chrome • Firefox • Opera • Microsoft Edge • Internet Explorer • Safari • Android
Action Timeout	Set the action timeout in seconds.

Field	Description
(seconds)	
Connection Persistence	Select an option for the connection persistence: <ul style="list-style-type: none"> • Standard - inherits the behavior with respect to the HTTP version (1.0 or 1.1). • Disabled - enforces connection closing following every HTTP message. • Enabled - enforces connection persistence through explicit keep-alive.
HTTP Version	Select the HTTP version used: <ul style="list-style-type: none"> • HTTP/1.0 • HTTP/1.1

TCP Settings

These parameters are configurable for both Client and Server settings, as presented in the following table.

Parameter	Description
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. 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. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
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). The default value is 1024.
Max source port	The Max value specifies the upper bound (the highest permissible port number). The default value is 65535.
Receive buffer size (bytes)	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.
Transmit buffer size (bytes)	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

Parameter	Description
	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.
RFC1323 TCP timestamps enabled	<p>Enable or disable the stamp using the toggle button. If enabled, the client or server inserts an RFC 1323 timestamp into each packet.</p> <p>NOTE Enabling the TCP Timestamp option adds 12 bytes to the TCP header. This reduces the effective configured MSS.</p>
Selective acknowledgments	<p>When enabled, the data receiver can inform the sender about all segments that have arrived successfully. Therefore, the sender will retransmit only the segments that have actually been lost.</p> <p>When disabled, the exchange of selective acknowledgments between the endpoints is no longer permitted. This is the default value.</p> <p>IMPORTANT Must be enabled for both client and server, to take effect. When running a mix of apps and attacks, attack profile's settings will be applied to both profiles, since it has the higher precedence.</p>

TLS Settings

NOTE TLS multi version support is available, you can configure both TLS 1.2 and TLS 1.3 from **Client TLS Settings**. You can choose multiple ciphers for each different version. The Client sends these versions and ciphers in the Client Hello and the Server chooses one of the versions and ciphers and replies back with Server Hello. The Client then proceeds with the handshake.

NOTE Once you select either of the two Session Reuse Methods below for the **Client TLS Settings**, you can specify how many simultaneous connections can share the same Session ID or Ticket through the **Session Reuse Count** option for **TLSv1.2**.

These parameters are configurable for both Client and Server settings, as presented in the following tables.

Client TLS Settings

Parameter	Description
	<i>Select this button to apply the client TLS settings configured at the currently selected application or attack level to the other existing application or attack profiles. When selecting this button, you are prompted to choose one or multiple client TLS profiles from the current configuration to which the current TLS settings will be applied.</i>
Enable TLS traffic	<p>IMPORTANT For Attacks traffic Profiles only.</p> <p>If enabled, the client will initiate all connections to the destination over TLS,</p>

Parameter	Description
	<p>based on the settings below. If disabled, connections will be established in plaintext.</p> <p>Even if Enable TLS traffic is not active, the client agent may use the TLS settings based on responses it receives from the server. For example, if the server sends an HTTP Redirect (3xx) response with a https:// URL, when the client agent follows that redirect, it will initiate a TLS connection based on the configured TLS settings.</p>
TLSv1.2	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>IMPORTANT Session reuse method is available only if TLSv1.2 is enabled.</p>
Session reuse count	<p>The number of simultaneous connections that can share the same Session ID or Session ticket.</p> <p>IMPORTANT This option appears only if client TLSv1.2 is enabled, and the Session reuse method is set to either the Session ticket or the Session ID method.</p>
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).
Send close notify	If enabled, it will send a close notify message.
TLSv1.3	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	This option is enabled by default. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).

Parameter	Description
Send close notify	If enabled, it will send a close notify message.

Server TLS Settings

Parameter	Description
	Select this button to apply the client TLS settings configured at the currently selected application or attack level to the other existing application or attack profiles. When selecting this button, you are prompted to choose one or multiple client TLS profiles from the current configuration to which the current TLS settings will be applied.
TLSv1.2	Select the check box to enable it. The following options became available:
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	Select the Session Reuse Method from the drop-down list: <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>NOTE Session reuse method is available only if TLSv1.2 is selected.</p>
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).
Send close notify	If enabled, it will send a close notify message.
TLSv1.3	Select the check box to enable it. The following options became available:
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.
SNI Enabled	Select the toggle button to enable the server name indicator. If enabled, the

Parameter	Description
	<i>following SNI Settings become available for each server name selected:</i>
Certificate file	Select Upload to add your certificate file or Clear to remove it.
Key file	Select Upload to add your key file or Clear to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select Upload to add your DH file or Clear to remove it.
Certificate file	Select Upload to add your certificate file or Clear to remove it.

RTP Settings

The following elements are available on the RTP Settings tab under the Traffic Profile Configuration section.

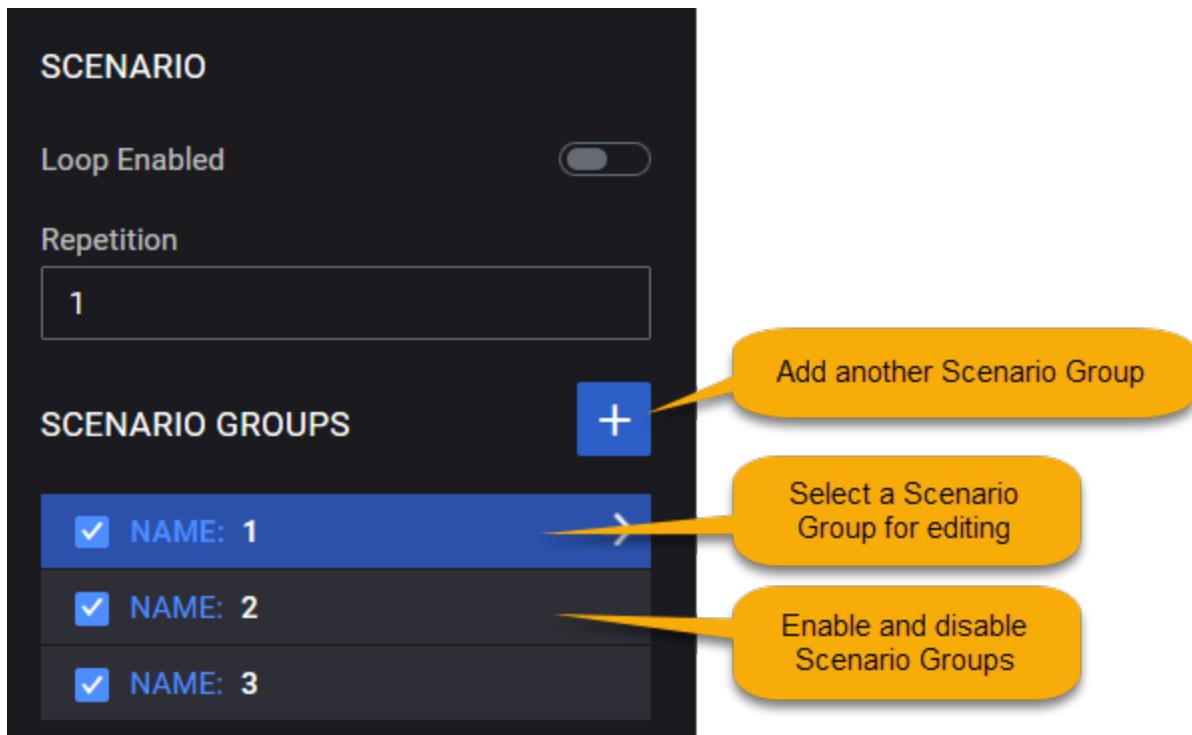
Settings	Description
Encryption Mode	Select an encryption mode from the drop-down list. Available options: None , XOR , ZOOM or SRTP .
MOS Mode	Select the Session Reuse Method from the drop-down list. Available options: Disable , Per interval or Per call .

CHAPTER 17

Scenario and Scenarion Groups 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 30](#) for detailed instructions.



A Cu Isolation *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.

When configuring Scenarios Groups, you also can configure the **Scenario** settings:

- **Loop Enabled** allows the configured scenarios to loop infinitely until the session times out.
- **Repetitions** value defines how many time the configured scenarios will be repeated.

Chapter contents:

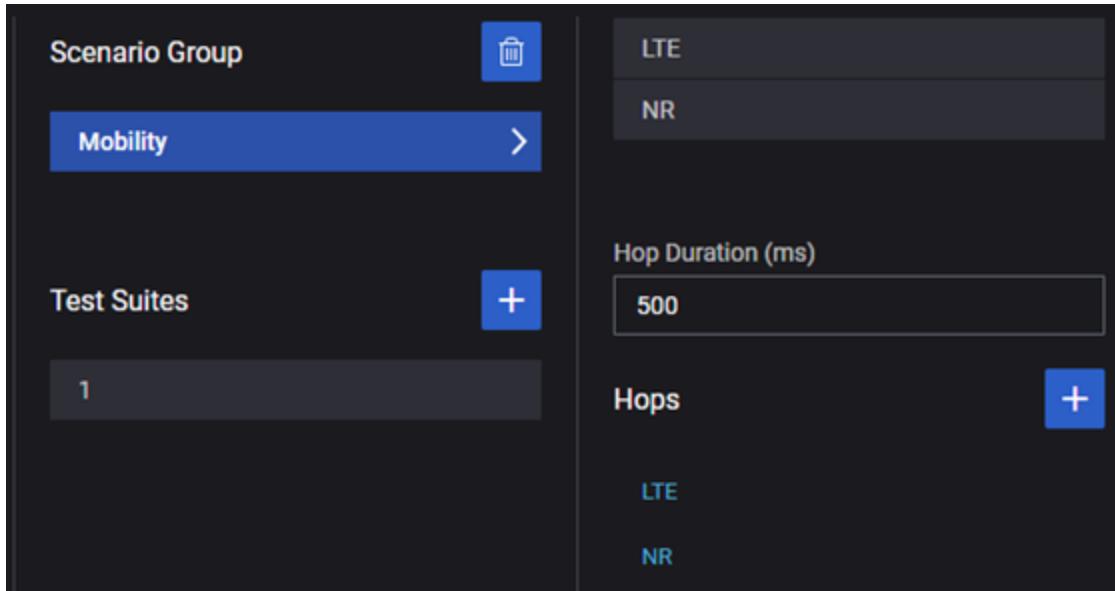
Mobility settings	336
Test Suite settings	339
Test procedures for SA	340
Deregistration	341
PDU Session Establish	342
PDU Session Release	344
Registration	346
Service Request	347
Test procedures for NSA tests	348
Attach	349
Detach	350
ENDC Configuration Update	351
EPS Bearer Activation	352
EPS Bearer Deactivation	353
Inter eNB Handover	354
PDN Connection Activation	355
PDN Connection Deactivation	357
SCG Release	359
SGNB Addition	360
MeNB Initiated SGNB Change Request	361
Test procedures for SA and NSA	362
Application Traffic	363
Delay	364
DU Initiated Release	365
NR-U Modification Request	366
UE Context Modification	367
IRAT Handover (LTE to NR)	368

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 32](#) (in the [Build and run a test on page 20](#) 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

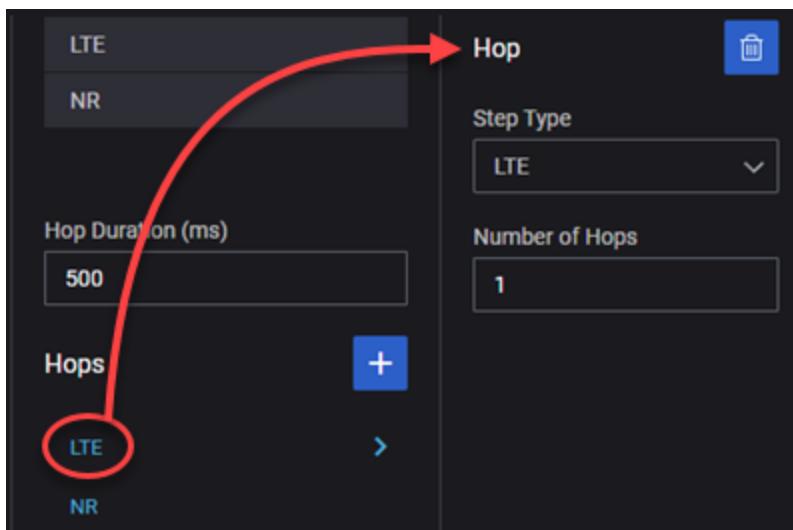
These are the settings that appear in the panel that opens when you select **Mobility** from the Scenario Group panel.

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. Cu Isolation adds an <i>NR</i> instance to the panel. When you click the instance, Cu Isolation 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, Cu Isolation changes the instance name to reflect that step type.
NR and LTE	When you click the Add Hop button, Cu Isolation 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 below.

Hops panel

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

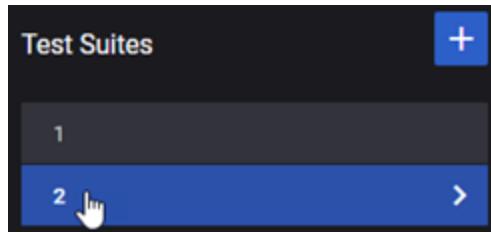


The following table describes the configuration settings in the Hops panel.

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.

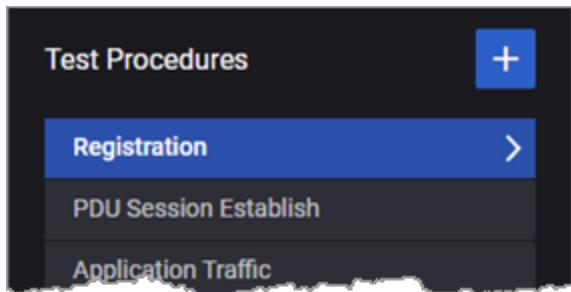
From a selected Scenario Group's **Test Suites** list, click an entry to open its **Test Suite** properties panel.

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, Cu Isolation 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, Cu Isolation calls each procedure in turn.</p> <p>Refer to Test procedures for SA on the facing page, Test procedures for NSA tests on page 348, and Test procedures for SA and NSA on page 362 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 362](#).

Procedure descriptions:

Deregistration	341
PDU Session Establish	342
PDU Session Release	344
Registration	346
Service Request	347

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 Cu Isolation 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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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	<p>The request type PDU session establishment:</p> <ul style="list-style-type: none"> • Initial Request: establish a new PDU Session. • Emergency: establish an emergency session with an Emergency APN.
PDU Type	<p>The Packet Data Unit (PDU) type to use for the PDU session. The available options are IPv4, IPv6, and IPv4v6.</p> <p>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).</p>
NRSM Info Transfer Flag	<p>This option specifies:</p> <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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 Release
<i>General:</i>	
Instance	Enter a value for this instance of the procedure.
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>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 Cu Isolation 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, Cu Isolation 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.

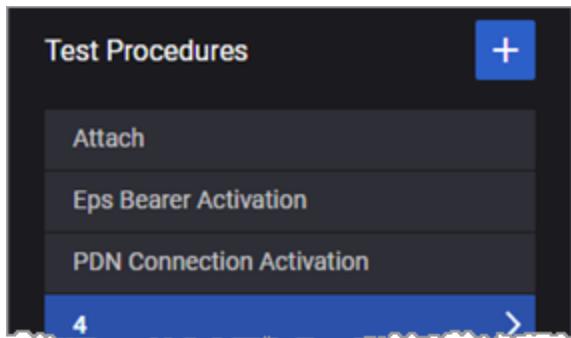
Configuration settings

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, Cu Isolation 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	<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>Emergency Services Fallback mode:</i>	
Service Type	<p>Select the service type:</p> <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 362](#).

Procedure descriptions:

Attach	349
Detach	350
ENDC Configuration Update	351
EPS Bearer Activation	352
EPS Bearer Deactivation	353
Inter eNB Handover	354
PDN Connection Activation	355
PDN Connection Deactivation	357
SCG Release	359
SGNB Addition	360
MeNB Initiated SGNB Change Request	361

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 Cu Isolation 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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 Attach.
<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.

Detach

This test procedure allows the simulated UEs to detach from the LTE network. Detach is the recommended last procedure in a defined Cu Isolation 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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 Detach
<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.

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 (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 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	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>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 Cu Isolation 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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 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	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>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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 Activation
<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>	
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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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	Enable this procedure if you are creating parallel (multi-threaded) procedures for this step in the call flow. Once you enable the option, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 SGNB Addition
<i>General Parameters:</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>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.

MeNB Initiated SGNB Change Request

This procedure is used in 5G networks where the Master eNodeB (MeNB) requests the Secondary gNodeB (SgNB) to modify the User Equipment (UE) context. This process is part of the dual connectivity feature, which allows a UE to be connected to both an LTE and a 5G NR network simultaneously, ensuring that the UE can maintain optimal connectivity and performance by dynamically adjusting its context based on network conditions and requirements.

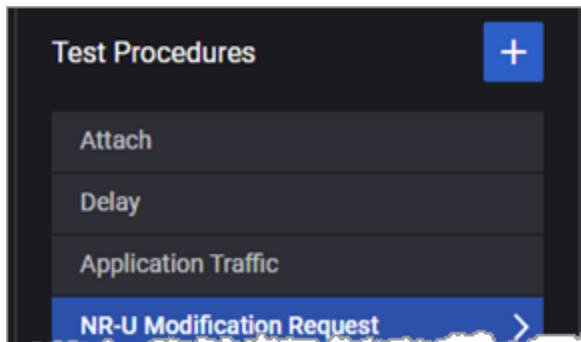
When MeNB sends an SGNB Modification Request message to the SgNB, the SgNB processes the request, making the necessary changes to the UE context.

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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 MeNB Initiated SGNB Change Request.
<i>General Parameters:</i>	
EPS Bearer ID	Select the bearers that have been changed and needs to be propagated. You can set the bearers from ID 5 to 15.
Target SCG CellId	Set the value for this parameter. When set as -1 , it allows the changes to be picked-up.

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	363
Delay	364
DU Initiated Release	365
NR-U Modification Request	366
UE Context Modification	367
IRAT Handover (LTE to NR)	368

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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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.

UE Context Modification

This procedure is used to update or modify the context of a User Equipment (UE). When CU sends a UE Context Modification Request to the DU, the DU processes this request making the necessary adjustments to the UE context.

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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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>	

Setting	Description
Procedure Type	Select UE Context Modification.
<i>General:</i>	
Cause	Select from the list the cause of modification in the message.
DRBS Required to Modify	Define the number of DRBs that needs to be modified.
DRBS Required to Release	Define the number of DRBs that needs to be released.
SRBS Required to Release	Define the number of SRBs that needs to be released.

IRAT Handover (LTE to NR)

Inter-Radio Access Technology (IRAT) Handover from LTE to NR (5G New Radio) procedure allows a mobile device to transition seamlessly from a 4G LTE network to a 5G NR network ensuring uninterrupted service and optimal performance.

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, Cu Isolation changes the panel to enable the definition of parallel procedures. Refer to Defining parallel procedures on page 36 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 IRAT HO.
<i>Properties:</i>	

Setting	Description
EPS Bearer List	Select the bearers that have been changed and needs to be propagated. You can set the bearers from ID 5 to 15.
Target SCG CellId	Set the value for this parameter. When set as -1 , it allows the changes to be picked-up.

CHAPTER 18

Manage and use test sessions

When you create a new test, Cu Isolation 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:

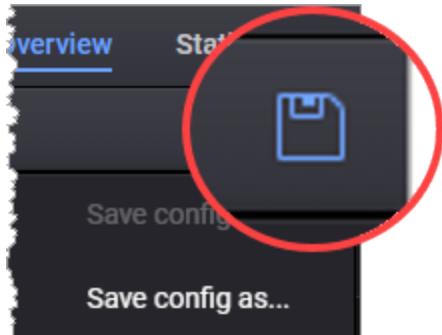
Save test sessions	371
Manage test sessions	372
Import and export sessions	376
Delete configs and sessions	378

Save test sessions

Once a test is configured (for details, refer to [Create a new test config on page 21](#)), you can record its configuration as a session, edit and save it for future use.

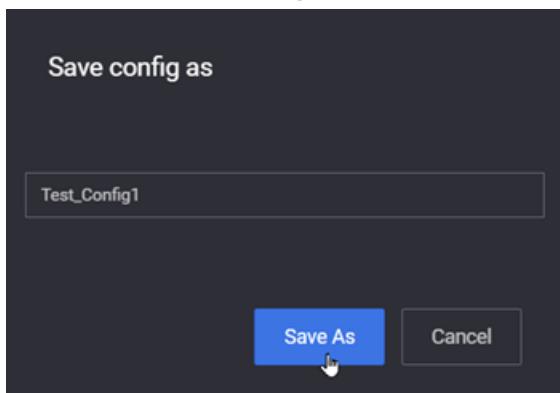
To save a configuration file, do the following:

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



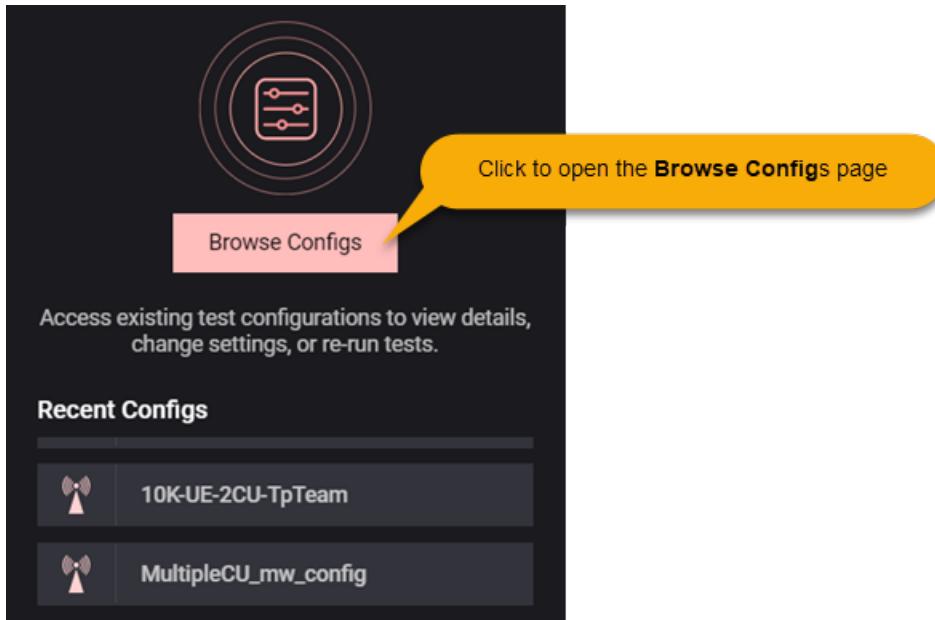
2. Choose one of the following:

- 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 Cu Isolation 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

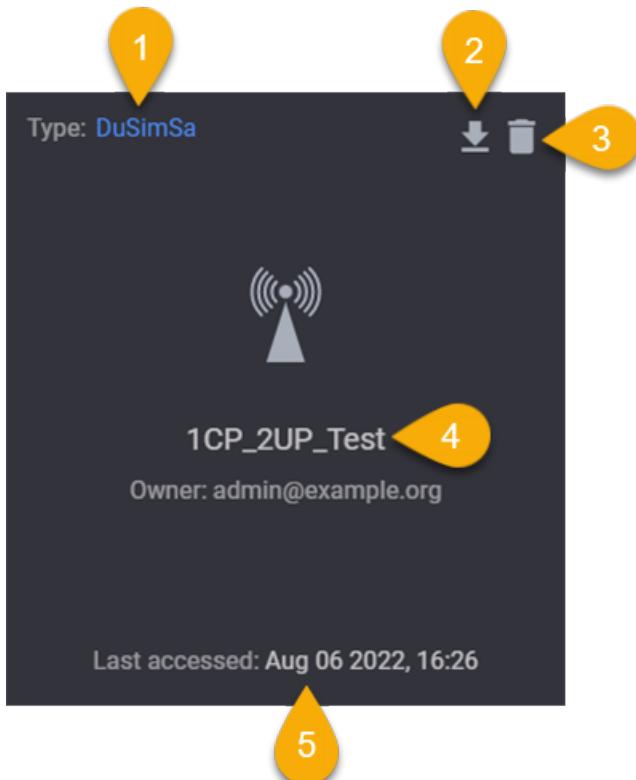
The **Recent Configs** category displays only the last twenty configurations in chronological order, the first being the most recent from all the categories listed above. In order to see all of your tests, you can display them sorted by category, by selecting a specific test category under **Recent Configs**.

Manage configurations

On this section,Cu Isolation 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

The screenshot shows a table with the following data:

Config Name	Last accessed	Application	Config Type	Owner	Create Session
SC_50Cell_UE4000	Aug 23, 2022, 1:26:22 PM	DuSimSa	admin@example.org	<input 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	<input type="checkbox"/>	

Buttons at the bottom left:

- Delete
- Export

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 NOTE For the base configurations, the test owner is <i>system</i> .
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.

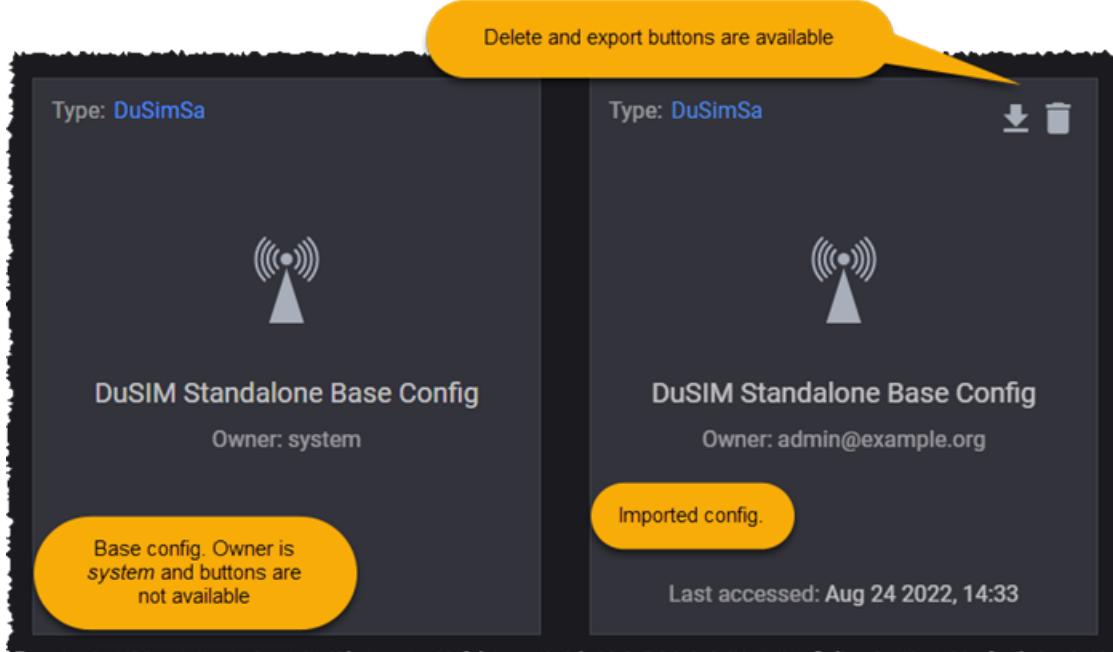


Import test configurations

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.

Config Name ↑	Last accessed ↓
<input type="checkbox"/> DuSIM Standalone Base Config (copy from Aug 24 11:38:15)	Aug 24, 2022, 2:38:15 PM
<input type="checkbox"/> DuSIM Standalone Base Config	The name of the test when it was imported the first time.
<input checked="" type="checkbox"/> 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 `Cu Isolation 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.

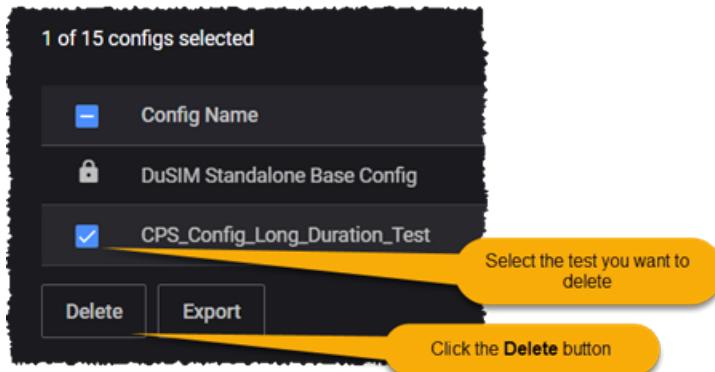
Delete configs and sessions

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.

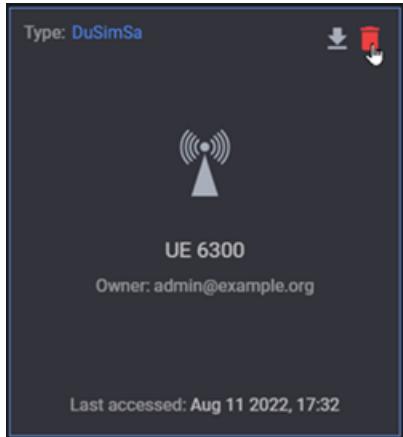
How to delete a Cu Isolation config

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:

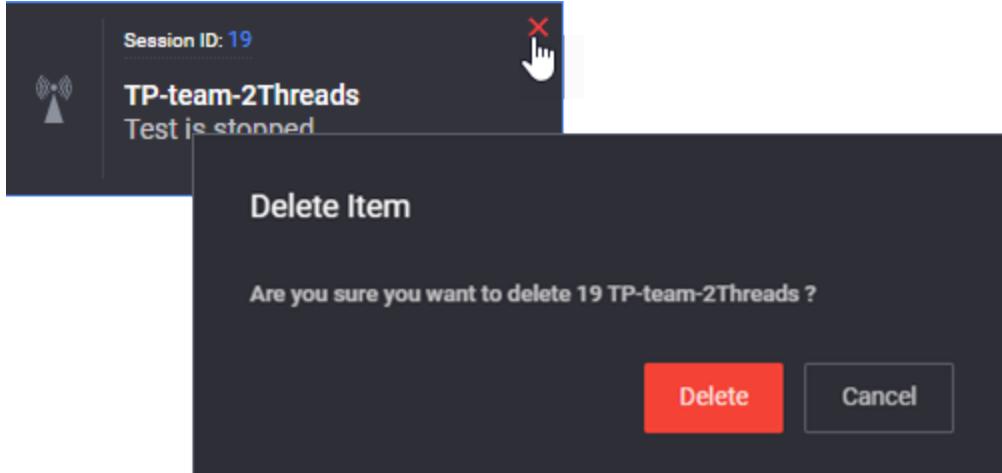
- The session will be permanently removed and cannot be recovered.
- However, when you delete a session, the session's config is not deleted. Therefore, you can create new sessions based on that config.

- 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 5.0 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 5.0 opens a confirmation dialog.



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

CHAPTER 19

Manage Cu Isolation licenses

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

Chapter contents:

Licensing Requirements	381
License Manager	382
License server	384

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 Cu Isolation web UI.

License Manager

The first time you use Cu Isolation, you need to activate at least one license. You activate and manage your licenses using the Cu Isolation **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 Cu Isolation License Manager:

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

Activate a license

To activate one or more Cu Isolation licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **Activate licenses**.
Cu Isolation 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 deactivate one or more Cu Isolation 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 Cu Isolation licenses:

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

Reserve a license

To reserve one or more Cu Isolation licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select the **Manage Reservation** icon.
Cu Isolation 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 Cu Isolation 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 Cu Isolation license operations:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **Offline operations**.
Cu Isolation 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 Cu Isolation 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 Cu Isolation web UI:

1. Log in the Cu Isolation 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 Cu Isolation web UI:

1. Log in the Cu Isolation 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 Cu Isolation licenses:

1. From the Setting menu (⚙), select **Application Settings**.
Cu Isolation 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 20

Manage Cu Isolation users

Managing the users who can access the application is one of the primary Cu Isolation 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 387](#)

User categories

Cu Isolation 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 Cu Isolation application must have a user account. To add a user:

1. Select the settings menu (⚙) and then select **User Management**.
Cu Isolation 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.
Cu Isolation 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.
Cu Isolation 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**.
Cu Isolation 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.
Cu Isolation 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:

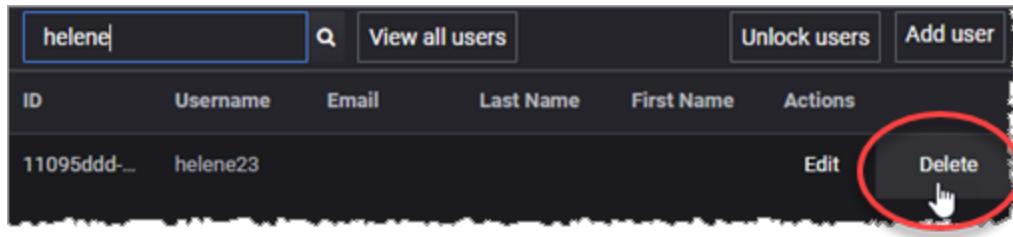
1. Select the settings menu () and then select **User Management**.
Cu Isolation opens the **Keycloak Admin Console** in a new browser tab.
2. Select **Users** from the list of **Manage** functions.
3. Select the user.
4. Set *User Enabled* to **OFF**.

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**.
Cu Isolation 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. Cu Isolation 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](#).

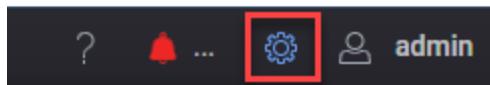
CHAPTER 21

Cu Isolation 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 390](#)
- [Events notifications on page 390](#)
- [Technical Support and Application Help on page 390](#)

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
Agent Management	Select this option to open the Agent management on page 78 window.
Application Settings	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 : <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 Cu Isolation MW. Refer to License Manager on page 382 for information about activating and managing licenses.
User Management	Application Administrators use the User Management settings for all aspects of user management. For detailed information, refer to Manage Cu Isolation users on page 385 .
Logs Level	You use the Logs Level setting to view and change the log level that it set for the Cu Isolation Controller. The logs level determines the type of data that are written to the log files:

Setting	Description
	<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.
Licensing > License Manager	Select this option to open the License Manager on page 382 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).
Data Migration	Allows you to export selected data (such as authentication data and configs) and to import controller data from a migrate package.
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.
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.

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 392](#) 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 394](#) for more information about collecting diagnostics data.

CHAPTER 22

Troubleshooting

Cu Isolation 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 Cu Isolation provides are notification and event management, messages displayed during test execution, test diagnostics data, and log files.

Chapter contents:

View Notifications and Test Events	392
Collect Diagnostics	394

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 Cu Isolation instance. The icon and the counter are visible from all the pages of the Cu Isolation 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		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 should either be restarted or should carry out error recovery or re-initialization routines.
WARNING		A <i>warning</i> notification indicates an error has occurred that potentially impacts application stability.
INFO		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.

Date	Type	Message
Aug 2, 2022, 10:13:53 AM	ERROR	The following agents are offline and cannot be rebooted: ...
Aug 2, 2022, 7:54:51 AM	INFO	CSV reports successfully generated for wireless-aa1623c...
Aug 2, 2022, 7:54:50 AM	INFO	Generating CSV reports for wireless-aa1623cc-bf11-4a16...
Aug 1, 2022, 5:40:59 PM	INFO	Licenses successfully activated
Aug 1, 2022, 5:06:34 PM	INFO	Sessions configs upgraded successfully. Refresh is neede...
Aug 1, 2022, 5:02:16 PM	ERROR	Could not get agents
Jul 30, 2022, 10:37:37 AM	INFO	PDF report successfully generated for wireless-7d81818e...
Jul 30, 2022, 10:37:23 AM	INFO	CSV reports successfully generated for wireless-7d81818...
Jul 30, 2022, 10:34:15 AM	INFO	Generating PDF report. Please note that this operation ma...

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.

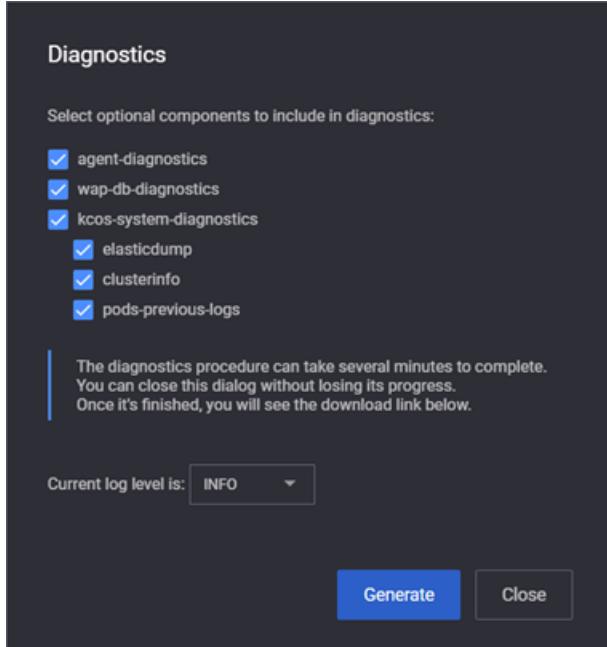
Filter events by			
Message	From	To	Notification type
<input type="text"/> Type keywords	<input type="button"/> Select a date	<input type="button"/> Select a date	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> i Info <input checked="" type="checkbox"/> ! Warning <input checked="" 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	i INFO	CSV reports successfully generated for wireless-de51d273-abfb-40f2-a9fb-ba353ce1f6e7.	
Aug 2, 2022, 10:52:24 AM	i 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	i INFO	CSV reports successfully generated for wireless-aa1623cc-bf11-4a16-9cf8-2ffff63aae01.	
Aug 2, 2022, 7:54:50 AM	i INFO	Generating CSV reports for wireless-aa1623cc-bf11-4a16-9cf8-2ffff63aae01.	
Aug 1, 2022, 5:40:59 PM	i INFO	Licenses successfully activated	

Collect Diagnostics

Cu Isolation 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.

APPENDIX A

Predefined Applications

The following table describes the available Predefined Applications.

Application	Description
Adobe Reader Updates Chrome	This application simulates Adobe Reader Updates web application with the Google Chrome browser.
Adobe Reader Updates Firefox	This application simulates Adobe Reader Updates web application with the Google Firefox browser.
Adobe Reader Updates Internet Explorer	This application simulates Adobe Reader Updates web application with the Google Internet Explorer browser.
Adobe Reader Updates Microsoft Edge	This application simulates Adobe Reader Updates web application with the Google Microsoft Edge browser.
ADP Chrome	This application simulates ADP web application with the Chrome browser.
ADP Firefox	This application simulates ADP web application with the Firefox browser.
ADP Internet Explorer	This application simulates ADP web application with the Internet Explorer browser.
ADP Microsoft Edge	This application simulates ADP web application with the Microsoft Edge browser.
Airbnb Chrome	This application simulates Airbnb web application with the Google Chrome browser.
Airbnb Firefox	This application simulates Airbnb web application with the Mozilla Firefox browser.
Airbnb Internet Explorer	This application simulates Airbnb web application with the Internet Explorer browser.
Airbnb Microsoft Edge	This application simulates Airbnb web application with the Microsoft Edge browser.
appointy Chrome	This application simulates appointy web application with the Chrome browser.
appointy Firefox	This application simulates appointy web application with the Firefox browser.
appointy Internet Explorer	This application simulates appointy web application with the Internet Explorer browser.
appointy Microsoft	This application simulates appointy web application with the Microsoft Edge browser.

Application	Description
Edge	browser.
AWS Console Chrome	This application simulates AWS Console web application with the Chrome browser.
AWS Console Firefox	This application simulates AWS Console web application with the Firefox browser.
AWS Console Internet Explorer	This application simulates AWS Console web application with the Internet Explorer browser.
AWS Console Microsoft Edge	This application simulates AWS Console web application with the Microsoft Edge browser.
AWS S3 Chrome	This application simulates AWS S3 web application with the Google Chrome browser.
AWS S3 Firefox	This application simulates AWS S3 web application with the Mozilla Firefox browser.
AWS S3 Internet Explorer	This application simulates AWS S3 web application with the Internet Explorer browser.
AWS S3 Microsoft Edge	This application simulates AWS S3 web application with the Microsoft Edge browser.
Baidu Chrome	This application simulates Baidu web application with the Chrome browser.
Baidu Firefox	This application simulates Baidu web application with the Firefox browser.
Baidu Internet Explorer	This application simulates Baidu web application with the Internet Explorer browser.
Baidu Maps Chrome	This application simulates Baidu Maps web application with the Google Chrome browser.
Baidu Maps Firefox	This application simulates Baidu Maps web application with the Mozilla Firefox browser.
Baidu Maps Internet Explorer	This application simulates Baidu Maps web application with the Internet Explorer browser.
Baidu Maps Microsoft Edge	This application simulates Baidu Maps web application with the Microsoft Edge browser.
Baidu Microsoft Edge	This application simulates Baidu web application with the Microsoft Edge browser.
Bilibili Chrome	This application simulates Bilibili web application with the Google Chrome browser.

Application	Description
Bilibili Firefox	This application simulates Bilibili web application with the Mozilla Firefox browser.
Bilibili Internet Explorer	This application simulates Bilibili web application with the Internet Explorer browser.
Bilibili Microsoft Edge	This application simulates Bilibili web application with the Microsoft Edge browser.
Cisco Spark Chrome	This application simulates Cisco Spark web application with the Chrome browser.
Cisco Spark Firefox	This application simulates Cisco Spark web application with the Firefox browser.
Cisco Spark Internet Explorer	This application simulates Cisco Spark web application with the Internet Explorer browser.
Cisco Spark Microsoft Edge	This application simulates Cisco Spark web application with the Microsoft Edge browser.
Commvault Chrome	This application simulates Commvault web application with the Google Chrome browser.
Commvault Firefox	This application simulates Commvault web application with the Mozilla Firefox browser.
Commvault Internet Explorer	This application simulates Commvault web application with the Internet Explorer browser.
Commvault Microsoft Edge	This application simulates Commvault web application with the Microsoft Edge browser.
Crawling Wikipedia (Chinese) Chrome	This application simulates Crawling Wikipedia (Chinese) web application with the Chrome browser.
Crawling Wikipedia (Chinese) Firefox	This application simulates Crawling Wikipedia (Chinese) web application with the Firefox browser
Crawling Wikipedia (Chinese) Internet Explorer	This application simulates Crawling Wikipedia (Chinese) web application with the Internet Explorer browser.
Crawling Wikipedia (Chinese) Microsoft Edge	This application simulates Crawling Wikipedia (Chinese) web application with the Microsoft Edge browser.

Application	Description
DocuSign Chrome	This application simulates DocuSign web application with the Google Chrome browser.
DocuSign Firefox	This application simulates DocuSign web application with the Mozilla Firefox browser.
DocuSign Internet Explorer	This application simulates DocuSign web application with the Internet Explorer browser.
DocuSign Microsoft Edge	This application simulates DocuSign web application with the Microsoft Edge browser.
Dreambox Chrome	This application simulates Dreambox web application with the Google Chrome browser.
Dreambox Firefox	This application simulates Dreambox web application with the Mozilla Firefox browser.
Dreambox Internet Explorer	This application simulates Dreambox web application with the Internet Explorer browser.
Dreambox Microsoft Edge	This application simulates Dreambox web application with the Microsoft Edge browser.
eBanking Chrome to Apache	This application simulates a banking web application with the Google Chrome browser connecting to an Apache web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Firefox to IIS	This application simulates a banking web application with the Mozilla Firefox browser connecting to an IIS web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Internet Explorer to Nginx	This application simulates a banking web application with the Internet Explorer browser connecting to an Nginx web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Microsoft Edge to Apache	This application simulates a banking web application with the Microsoft Edge browser connecting to an Apache web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
EpixNow Chrome	This application simulates EpixNow web application with the Google Chrome browser.
EpixNow Firefox	This application simulates EpixNow web application with the Mozilla Firefox browser.

Application	Description
EpixNow Internet Explorer	This application simulates EpixNow web application with the Internet Explorer browser.
EpixNow Microsoft Edge	This application simulates EpixNow web application with the Microsoft Edge browser.
eShop Chrome to Apache	This application simulates an online shop web application with the Google Chrome browser connecting to an Apache web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Firefox to IIS	This application simulates an online shop web application with the Mozilla Firefox browser connecting to an IIS web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Internet Explorer to Nginx	This application simulates an online shop web application with the Internet Explorer browser connecting to an Nginx web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Microsoft Edge to Apache	This application simulates an online shop web application with the Microsoft Edge browser connecting to an Apache web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
Facebook Audio Chrome	This application simulates Facebook Audio web application with the Google Chrome browser.
Facebook Audio Firefox	This application simulates Facebook Audio web application with the Mozilla Firefox browser.
Facebook Audio Internet Explorer	This application simulates Facebook Audio web application with the Internet Explorer browser.
Facebook Audio Microsoft Edge	This application simulates Facebook Audio web application with the Microsoft Edge browser.
Facebook Chrome	This application simulates Facebook web application with the Google Chrome browser.
Facebook Firefox	This application simulates Facebook web application with the Mozilla Firefox browser.
Facebook Internet Explorer	This application simulates Facebook web application with the Internet Explorer browser.
Facebook Microsoft Edge	This application simulates Facebook web application with the Microsoft Edge browser.

Application	Description
FacebookLive Chrome	This application simulates FacebookLive web application with the Google Chrome browser.
FacebookLive Firefox	This application simulates FacebookLive web application with the Mozilla Firefox browser.
FacebookLive Internet Explorer	This application simulates FacebookLive web application with the Internet Explorer browser.
FacebookLive Microsoft Edge	This application simulates FacebookLive web application with the Microsoft Edge browser.
Gab Chrome	This application simulates Gab web application with the Google Chrome browser.
Gab Firefox	This application simulates Gab web application with the Mozilla Firefox browser.
Gab Internet Explorer	This application simulates Gab web application with the Internet Explorer browser.
Gab Microsoft Edge	This application simulates Gab web application with the Microsoft Edge browser.
Gaode Maps Chrome	This application simulates Gaode Maps web application with the Google Chrome browser.
Gaode Maps Firefox	This application simulates Gaode Maps web application with the Mozilla Firefox browser.
Gaode Maps Internet Explorer	This application simulates Gaode Maps web application with the Internet Explorer browser.
Gaode Maps Microsoft Edge	This application simulates Gaode Maps web application with the Microsoft Edge browser.
Google Classroom Chrome	This application simulates Google Classroom web application with the Chrome browser.
Google Classroom Firefox	This application simulates Google Classroom web application with the Firefox browser.
Google Classroom Internet Explorer	This application simulates Google Classroom web application with the Internet Explorer browser.
Google Classroom Microsoft Edge	This application simulates Google Classroom web application with the Microsoft Edge browser.
Google Drive Chrome	This application simulates Google Drive web application with the Google Chrome browser.

Application	Description
Google Drive Firefox	This application simulates Google Drive web application with the Mozilla Firefox browser.
Google Drive Internet Explorer	This application simulates Google Drive web application with the Internet Explorer browser.
Google Drive Microsoft Edge	This application simulates Google Drive web application with the Microsoft Edge browser.
Google Sheets Chrome	This application simulates Google Sheets web application with the Chrome browser.
Google Sheets Firefox	This application simulates Google Sheets web application with the Firefox browser.
Google Sheets Internet Explorer	This application simulates Google Sheets web application with the Internet Explorer browser.
Google Sheets Microsoft Edge	This application simulates Google Sheets web application with the Microsoft Edge browser.
Google Slides Chrome	This application simulates Google Slides web application with the Chrome browser.
Google Slides Firefox	This application simulates Google Slides web application with the Firefox browser.
Google Slides Internet Explorer	This application simulates Google Slides web application with the Internet Explorer browser.
Google Slides Microsoft Edge	This application simulates Google Slides web application with the Microsoft Edge browser.
GoogleHangouts Chrome	This application simulates GoogleHangouts web application with the Chrome browser.
GoogleHangouts Firefox	This application simulates GoogleHangouts web application with the Firefox browser.
GoogleHangouts Internet Explorer	This application simulates GoogleHangouts web application with the Internet Explorer browser.
GoogleHangouts Microsoft Edge	This application simulates GoogleHangouts web application with the Microsoft Edge browser.
GooglePhotos Chrome	This application simulates GooglePhotos web application with the Chrome browser.
GooglePhotos Firefox	This application simulates GooglePhotos web application with the Firefox browser.

Application	Description
GooglePhotos Internet Explorer	This application simulates GooglePhotos web application with the Internet Explorer browser.
GooglePhotos Microsoft Edge	This application simulates GooglePhotos web application with the Microsoft Edge browser.
HTTP App	This application simulates a generic HTTP application.
Jingdong Chrome	This application simulates Jingdong web application with the Google Chrome browser.
Jingdong Firefox	This application simulates Jingdong web application with the Mozilla Firefox browser.
Jingdong Internet Explorer	This application simulates Jingdong web application with the Internet Explorer browser.
Jingdong Microsoft Edge	This application simulates Jingdong web application with the Microsoft Edge browser.
Jira Chrome	This application simulates Jira web application with the Chrome browser.
Jira Firefox	This application simulates Jira web application with the Firefox browser.
Jira Internet Explorer	This application simulates Jira web application with the Internet Explorer browser.
Jira Microsoft Edge	This application simulates Jira web application with the Microsoft Edge browser.
League of Legends Chrome	This application simulates League of Legends web application with the Google Chrome browser.
League of Legends Firefox	This application simulates League of Legends web application with the Mozilla Firefox browser.
League of Legends Internet Explorer	This application simulates League of Legends web application with the Internet Explorer browser.
League of Legends Microsoft Edge	This application simulates League of Legends web application with the Microsoft Edge browser.
Mail.ru Chrome	This application simulates Mail.ru web application with the Chrome browser.
Mail.ru Firefox	This application simulates Mail.ru web application with the Firefox browser.
Mail.ru Internet Explorer	This application simulates Mail.ru web application with the Internet Explorer browser.
Mail.ru Microsoft Edge	This application simulates Mail.ru web application with the Microsoft Edge browser.

Application	Description
Meraki Chrome	This application simulates Meraki web application with the Google Chrome browser.
Meraki Firefox	This application simulates Meraki web application with the Mozilla Firefox browser.
Meraki Internet Explorer	This application simulates Meraki web application with the Internet Explorer browser.
Meraki Microsoft Edge	This application simulates Meraki web application with the Microsoft Edge browser.
Mewe Chrome	This application simulates Mewe web application with the Google Chrome browser.
Mewe Firefox	This application simulates Mewe web application with the Mozilla Firefox browser.
Mewe Internet Explorer	This application simulates Mewe web application with the Internet Explorer browser.
Mewe Microsoft Edge	This application simulates Mewe web application with the Microsoft Edge browser.
MongoDB	This application simulates the MongoDB, a cross-platform document-oriented database.
Netease Music Chrome	This application simulates Netease Music web application with the Google Chrome browser.
Netease Music Firefox	This application simulates Netease Music web application with the Mozilla Firefox browser.
Netease Music Internet Explorer	This application simulates Netease Music web application with the Internet Explorer browser.
Netease Music Microsoft Edge	This application simulates Netease Music web application with the Microsoft Edge browser.
Office 365 Outlook People Chrome	This application simulates Office 365 Outlook People web application with the Chrome browser.
Office 365 Outlook People Firefox	This application simulates Office 365 Outlook People web application with the Firefox browser.
Office 365 Outlook People Internet Explorer	This application simulates Office 365 Outlook People web application with the Internet Explorer browser.
Office 365 Outlook	This application simulates Office 365 Outlook People web application with the

Application	Description
People Microsoft Edge	Microsoft Edge browser.
Office365 Excel Chrome	This application simulates Office365 Excel web application with the Google Chrome browser.
Office365 Excel Firefox	This application simulates Office365 Excel web application with the Mozilla Firefox browser.
Office365 Excel Internet Explorer	This application simulates Office365 Excel web application with the Internet Explorer browser.
Office365 Excel Microsoft Edge	This application simulates Office365 Excel web application with the Microsoft Edge browser.
Office365 OneDrive Chrome	This application simulates Office365 OneDrive web application with the Google Chrome browser.
Office365 OneDrive Firefox	This application simulates Office365 OneDrive web application with the Mozilla Firefox browser.
Office365 OneDrive Internet Explorer	This application simulates Office365 OneDrive web application with the Internet Explorer browser.
Office365 OneDrive Microsoft Edge	This application simulates Office365 OneDrive web application with the Microsoft Edge browser.
Office365 Outlook Chrome	This application simulates Office365 Outlook web application with the Google Chrome browser.
Office365 Outlook Firefox	This application simulates Office365 Outlook web application with the Mozilla Firefox browser.
Office365 Outlook Internet Explorer	This application simulates Office365 Outlook web application with the Internet Explorer browser.
Office365 Outlook Microsoft Edge	This application simulates Office365 Outlook web application with the Microsoft Edge browser.
OK.ru Chrome	This application simulates OK.ru web application with the Chrome browser.
OK.ru Firefox	This application simulates OK.ru web application with the Firefox browser.
OK.ru Internet Explorer	This application simulates OK.ru web application with the Internet Explorer browser.
OK.ru Microsoft Edge	This application simulates OK.ru web application with the Microsoft Edge browser.

Application	Description
Portal Chrome to Apache	This application simulates a portal web application with the Google Chrome browser connecting to an Apache web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Firefox to IIS	This application simulates a portal web application with the Mozilla Firefox browser connecting to an IIS web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Internet Explorer to Nginx	This application simulates a portal web application with the Internet Explorer browser connecting to an Nginx web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Microsoft Edge to Apache	This application simulates a portal web application with the Microsoft Edge browser connecting to an Apache web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Reddit Chrome	This application simulates Reddit web application with the Google Chrome browser.
Reddit Firefox	This application simulates Reddit web application with the Mozilla Firefox browser.
Reddit Internet Explorer	This application simulates Reddit web application with the Internet Explorer browser.
Reddit Microsoft Edge	This application simulates Reddit web application with the Microsoft Edge browser.
Salesforce Chrome	This application simulates Salesforce web application with the Chrome browser.
Salesforce Firefox	This application simulates Salesforce web application with the Firefox browser.
Salesforce Internet Explorer	This application simulates Salesforce web application with the Internet Explorer browser.
Salesforce Microsoft Edge	This application simulates Salesforce web application with the Microsoft Edge browser.
Service-Now Chrome	This application simulates Service-Now web application with the Google Chrome browser.
Service-Now Firefox	This application simulates Service-Now web application with the Mozilla Firefox browser.
Service-Now	This application simulates Service-Now web application with the Internet

Application	Description
Internet Explorer	Explorer browser.
Service-Now Microsoft Edge	This application simulates Service-Now web application with the Microsoft Edge browser.
Skype 8 Chrome	This application simulates Skype 8 web application with the Chrome browser.
Skype 8 Firefox	This application simulates Skype 8 web application with the Firefox browser.
Skype 8 Internet Explorer	This application simulates Skype 8 web application with the Internet Explorer browser.
Skype 8 Microsoft Edge	This application simulates Skype 8 web application with the Microsoft Edge browser.
Skype Chrome	This application simulates Skype web application with the Chrome browser.
Skype Firefox	This application simulates Skype web application with the Firefox browser.
Skype Internet Explorer	This application simulates Skype web application with the Internet Explorer browser.
Skype Microsoft Edge	This application simulates Skype web application with the Microsoft Edge browser.
SMTP	Emulates an SMTP Email session.
Social Network Chrome to Apache	This application simulates a social network web application with Google Chrome browser connecting to an Apache web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Firefox to IIS	This application simulates a social network web application with Mozilla Firefox browser connecting to an IIS web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Internet Explorer to Nginx	This application simulates a social network web application with Internet Explorer browser connecting to an Nginx web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Microsoft Edge to Apache	This application simulates a social network web application with Microsoft Edge browser connecting to an Apache web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Splunk Chrome	This application simulates Splunk web application with the Google Chrome browser.

Application	Description
Splunk Firefox	This application simulates Splunk web application with the Mozilla Firefox browser.
Splunk Internet Explorer	This application simulates Splunk web application with the Internet Explorer browser.
Splunk Microsoft Edge	This application simulates Splunk web application with the Microsoft Edge browser.
Tubi Chrome	This application simulates Tubi web application with the Chrome browser.
Tubi Firefox	This application simulates Tubi web application with the Firefox browser.
TWC Firefox	This application simulates TWC web application with the Firefox browser.
TWC Internet Explorer	This application simulates TWC web application with the Internet Explorer browser.
TWC Microsoft Edge	This application simulates TWC web application with the Microsoft Edge browser.
Video Platform Chrome to Apache	This application simulates a video platform web application with Google Chrome browser connecting to an Apache web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Firefox to IIS	This application simulates a video platform web application with Mozilla Firefox browser connecting to an IIS web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Internet Explorer to Nginx	This application simulates a video platform web application with Internet Explorer browser connecting to an Nginx web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Microsoft Edge to Apache	This application simulates a video platform web application with Microsoft Edge browser connecting to an Apache web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
VKontakte Chrome	This application simulates VKontakte web application with the Chrome browser.
VKontakte Firefox	This application simulates VKontakte web application with the Firefox browser.
VKontakte Internet Explorer	This application simulates VKontakte web application with the Internet Explorer browser.

Application	Description
Vkontakte Microsoft Edge	This application simulates VKontakte web application with the Microsoft Edge browser.
Yammer Chrome	This application simulates Yammer web application with the Google Chrome browser.
Yammer Firefox	This application simulates Yammer web application with the Mozilla Firefox browser.
Yammer Internet Explorer	This application simulates Yammer web application with the Internet Explorer browser.
Yammer Microsoft Edge	This application simulates Yammer web application with the Microsoft Edge browser.
YYLive Chrome	This application simulates YYLive web application with the Google Chrome browser.
YYLive Firefox	This application simulates YYLive web application with the Mozilla Firefox browser.
YYLive Internet Explorer	This application simulates YYLive web application with the Internet Explorer browser.
YYLive Microsoft Edge	This application simulates YYLive web application with the Microsoft Edge browser.

APPENDIX B**Cu IsolationApplication Actions**

The following table lists the application actions and action parameters available in Cu Isolation.

Application Action	Action Parameters	Parameter Description
<i>Adobe Reader Updates</i>		
Check For Updates	Current Version	Displays the current version.
	Update Version	Displays the update version.
Download Updates	Update Version	Displays the current version.
<i>ADP</i>		
Load Main Paige	N/A	N/A
Load Login Information Page	N/A	N/A
Load Employee Login Page	N/A	N/A
<i>Airbnb</i>		
Load First Page	City	Set the city name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
Specify Search Criteria	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Second selected rental	Set the second selected rental name.

Application Action	Action Parameters	Parameter Description
Select a Rental	Main rental photo	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Main rental photo (low resolution)	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo of host	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 2 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 3 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 4 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Photo 5 of rental		<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Airbnb host name	Set the airbnb host name.
	Reviewer	Set the reviewer name.
	Second reviewer	Set the second reviewer name.
	Third reviewer	Set the third reviewer name.
View Rental Photos	Thumbnail photo of host	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Thumbnail photo of first reviewer	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Thumbnail photo of third reviewer	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.

Application Action	Action Parameters	Parameter Description
	Checkout Date	Set the check-out date.
View More Amenities	City	Set the city name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
View Hot Profile	Thumbnail photo of first reviewer	
View Second Property	Photo 3 of rental	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Airbnb host name	Set the airbnb host name.
	Reviewer	Set the reviewer name.
	Second reviewer	Set the second reviewer name.
	Third reviewer	Set the third reviewer name.
	Second selected rental	Set the second selected rental name.
	Photo 1 of rental	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
	Photo 4 of rental	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 5 of rental	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	Second selected rental	Set the second selected rental name.
View the Calendar	N/A	N/A
<i>appointy</i>		
Load Login Page	User name	Set the user name.
Login	User name	Set the user name.
	Password	Provide the password
	Profession	Set the profession.
	City	Set the city name.
	State/Province	Set the state/province name.
	Staff member 1	Set the name of the first staff member.
	Staff member 2	Set the name of the second staff member.
	Customer 1 first name	Set the first name of Customer 1.
	Customer 1 last name	Set the last name of Customer 1.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.

Application Action	Action Parameters	Parameter Description
Book New Customer	User name	Set the user name.
	Full manager name	Set the manager name.
	City	Set the city name.
	State/Province	Set the state/province name.
	Service	Set the service name.
	Staff member 1	Set the name of the first staff member.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.
View New Users Pulldown	User name	Set the user name.
View New Appointments Pulldown	User name	Set the user name.
Select Dashboard Tab	User name	Set the user name.
	Profession	Set the profession.
Select Reports Tab	User name	Set the user name.
View Week Calendar	User name	Set the user name.
View Customers Tab	User name	Set the user name.
	City	Set the city name.
	Customer 1 first name	Set the first name of Customer 1.
	Customer 1 last name	Set the last name of Customer 1.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.

Application Action	Action Parameters	Parameter Description
Logout	User name	Set the user name.
<i>AWS Console</i>		
Load AWS Page	N/A	N/A
Load AWS Management Console	Region name	Set the region name.
Sign In	User email	Provide the user email.
	Password	Provide the password.
	User name	Set the user name.
	Region name	Set the region name.
Check Account Info	User email	Provide the user email.
	Region name	Set the region name.
Check Account Billing	User email	Provide the user email.
	Region name	Set the region name.
Check Credentials	Region name	Set the region name.
	Existing keyID 1	Provide the existing keyID 1.
	Existing keyID 2	Provide the existing keyID 2.
Create New Access Key	New KeyID	Set the new keyID.
Download Key file	New KeyID	Set the new keyID.
	Key file name	Set the key file name.
Delete Key	Existing keyID 1	Provide the existing keyID 1.
Sign Out	User email	Provide the user email.
	Region name	Set the region name.
<i>AWS S3</i>		

Application Action	Action Parameters	Parameter Description
Check Buckets Names	User email	Provide the user email.
	Region name	Set the region name.
	KeyID	Provide the keyID.
Create Buckets	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
Upload File	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket bame	Set the source bucket name.
	Local file name for upload	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
List Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Source file name	Set the source file name.
Copy Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
	Source file name	Set the source file name.

Application Action	Action Parameters	Parameter Description
Verify Copied Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Destination bucket name	Set the destination bucket name.
Download Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Source file name	Set the source file name.
Delete Files and Buckest	User email	Provide the user email.
	Region name	Set the region name.
	KeyID	Provide the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
	Source file name	Set the source file name.
<i>Baidu</i>		
Access Baidu News	N/A	N/A
Access Baidu Maps	N/A	N/A
Access Baidu Pictures	N/A	N/A
Load Maine Paige	N/A	N/A
Search String	Search query	Provide the search criteria.
Search Image	Baidu search image file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
Access Baidu Passport	N/A	N/A
<i>Baidu Maps</i>		
Load Web Page	N/A	N/A
Search a Place	Query string	Provide the search criteria.
Finding a route	Query string	Provide the search criteria.
	Source location	Set the search location.
	Destination location	Set the destination location.
<i>Bilibili</i>		
Open Bilibili Website	N/A	N/A
Login	Username	Provide the username.
	Password	Provide the password.
Search Video	Video name	Provide the video name.
Watch Video	N/A	N/A
Upload Video	Uploaded video title	Set the title for the uploaded video.
	Uploaded video file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout	N/A	N/A
<i>Cisco Spark</i>		
Start the Application	N/A	N/A
Click Get Started	N/A	N/A
Click Next	User email address	Provide the user's email address.
Click SignIn	The contact's	Provide the contact's first/last name.

Application Action	Action Parameters	Parameter Description
	first/last name	
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
	Password	Provide the password.
	User's first/last name	Provide the user's first/last name
Create a Team	User email address	Provide the user's email address.
Add Contact	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Send Message	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Send File	User email address	Provide the user's email address.
	User's first/last name	Provide the user's first/last name
Initiate a Call	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.

Application Action	Action Parameters	Parameter Description
Hang Up Call	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Exit	N/A	N/A
<i>Commvault</i>		
Get Login Page	N/A	N/A
Login	User email	Provide the user's email address.
	Password	Provide the password.
View Drive	N/A	N/A
Create Folder	Created folder name	Set the name of the created folder.
Rename Folder	Folder name	Set the folder's new name.
Move File	Folder name	Provide the folder name.
Navigate To Folder	Folder name	Provide the folder name.
Upload File	Uploaded file name	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Download File	Downloaded file name	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Get Public Link	Folder ID	Provide the folder ID.
Move File To Trash	N/A	N/A
View Trash	N/A	N/A

Application Action	Action Parameters	Parameter Description
Restore File From Trash	Folder name	Provide the folder name.
Empty Trash	N/A	N/A
View Public Links	N/A	N/A
Deelte Public Link	Folder ID	Provide the folder ID.
Log Out	N/A	N/A
<i>Crawling Wikipedia (Chinese)</i>		
Crawl Link 1	Root URI	Set the root URI.
Crawl Link 2	Root URI	Set the root URI.
Crawl Link 3	Root URI	Set the root URI.
Crawl Link 4	Root URI	Set the root URI.
<i>DocuSign</i>		
Load Front Page	N/A	N/A
<i>Dreambox</i>		
Login	Login email address	Provide the login email address.
	Password	Provide the password.
Open Dashboard	N/A	N/A
Check Activity Status	From date	Set the starting date.
	To date	Set the end date.
Add Assignment	Select a grade	Set a grade.
	Select a category	Set a category.
	Short description	provide a short description.
Set Dreambox Game	N/A	N/A
Pause Dreambox Game	N/A	N/A
Quit Dreambox	N/A	N/A

Application Action	Action Parameters	Parameter Description
Game		
Logout	N/A	N/A
<i>eBanking</i>		
Sign Up	SignUp username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	SignUp password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	SignUp confirm password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Login	Login username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
View Transactions	N/A	N/A
View Accounts	N/A	N/A
Get Contact Page	N/A	N/A
Logout	N/A	N/A
<i>EpixNow</i>		

Application Action	Action Parameters	Parameter Description
Open Login Page	N/A	N/A
Login	Email	Provide the login email address.
	Password	Provide the password.
Browse Movies	Search keyword	Provide the search criteria.
Search Movies	Search keyword	Provide the search criteria.
Play	Search keyword	Provide the search criteria.
Logout	N/A	N/A
<i>eShop</i>		
Search Product	Product name	Provide the product name.
View Product	Product ID	Provide the product ID.
Login	Login username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Add To Cart	N/A	N/A
Remove From Cart	N/A	N/A
Buy	Full name	Provide the full name.
	Address	Provide the address.
	Account number	Provide the account number.
Logout	N/A	N/A
<i>Facebook Audio</i>		
Open Home Page	N/A	N/A
Login	Encrypted	Provide the password.

Application Action	Action Parameters	Parameter Description
	password	
	Email	Provide the login email address.
Create Audio Room	N/A	N/A
Join Audio Room	N/A	N/A
Leave Audio Room	N/A	N/A
Logout	N/A	N/A
<i>Facebook</i>		
Get Homepage	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User first name	Provide the first name.
	User second name	Provide the second name.
Open Notifications	N/A	N/A
Search Person	Search string	Provide the search criteria.
Add Friend	Friend first name	Provide the friend's first name.
	Friend second name	Provide the friend's second name.
Send Message	Message body	Provide the message.
	Recipient first name	Provide the recipient's first name.
	Recipient second name	Provide the recipient's second name.

Application Action	Action Parameters	Parameter Description
Send Message With Attachment	Message body	Provide the message.
	Recipient first name	Provide the recipient's first name.
	Recipient second name	Provide the recipient's second name.
	Filename	Provide the file name
	Upload File	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Download Attachment	Download file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Go To Profile	N/A	N/A
Post In News Feed	Post Message	Provide the message.
	Post file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Comment Post	Comment message	Provide the post message.
	Post author	Provide the post's author.
Delete Comment	Post author	Provide the post's author.
Like Post	N/A	N/A
Unlike Post	N/A	N/A
Sign Out	N/A	N/A
<i>FacebookLive</i>		

Application Action	Action Parameters	Parameter Description
Sign In	C_user cookie2	Set the value.
	C_user cookie	Set the value.
	User email address	Provide the user email address.
	Password	Provide the password.
	User name	Provide the username.
	Friend 1 first name	Provide the first name.
Start Live Stream	C_user cookie	Set the value.
	User name	Provide the username.
	Friend 1 first name	Provide the first name.
	Friend 3 first name	Provide the first name.
	Video stream ID	Set the video stream ID.
Sign Out	C_user cookie	Set the value.
	User email address	Provide the user email address.
	User name	Provide the username.
	Video stream ID	Set the video stream ID.
<i>Gab</i>		
Open Home Page	N/A	N/A
Open Login Page	N/A	N/A
Login	Email	Provide the email address.
	Password	Provide the password.
Read News	N/A	N/A
Post News	Statut text	Provide the message.
Logout	N/A	N/A

Application Action	Action Parameters	Parameter Description
<i>Gaode Maps</i>		
Open Website	N/A	N/A
Search Location	Destination	Provide the destination.
Find Route	Destination	Provide the destination.
	Starting location	Provide the starting location.
	Transportation method	Provide the transportation method.
<i>Google Classroom</i>		
Load Homepage	N/A	N/A
Login	Username	Provide the username.
	User email	Provide the email address.
	User password	Provide the password.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
Create New Classroom	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Create New Post	Post text	Provide the text message.
Edit Post	Post text	Provide the text message.
Add Attachment to Post	Post attachment	Select an option:

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Post text	Provide the text message.
Load Classroom Tab	N/A	N/A
Create New Assignment	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Add Attachment to Assignment	Assignment document	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Assignment title	Provide the assignment title.
Load People Tab	N/A	N/A
Invite a Student	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.

Application Action	Action Parameters	Parameter Description
Student Load Homepage	Post attachment	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Student Add Submission	Submission document compressed	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Add Student Private Comment	Student private comment	Provide the comment.
Load Grades Tab	Assignment title	Provide the assignment title.

Application Action	Action Parameters	Parameter Description
View Submission	Submission document	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Submission document webp format	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Assignment title	Provide the assignment title.
	Student private comment	Provide the comment.
Add Professor Private Comment	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Assignment title	Provide the assignment title.
	Student private comment	Provide the comment.
	Professor private comment	Provide the comment.
Grade Submission	Grade of the	Provide the grade value.

Application Action	Action Parameters	Parameter Description
	assignment	
Archive Classroom	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Delete Classroom	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Logout	Username	Provide the username.
	User email	Provide the email address.
<i>Google Drive</i>		
Get Sigh In Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Create Folder	Folder name	Set the folder name.
Upload File	File name	Provide the file name.
	Upload file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Delete File	File name	Provide the file name.
Empty Bin	File name	Provide the file name.
	File content	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Create Text Document	Document content	Provide the document content.
	Document name	Provide the document name.
Create Presentation	Powerpoint content	Provide the content.
	Powerpoint name	Provide the name.
Create Spreadsheet	Spreadsheet content	Provide the content.
	Spreadsheet name	Provide the name.
Download File	File name	Provide the file name.
	Downloaded file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Sign Out	N/A	N/A
<i>Google Sheets</i>		
Load Sigh In Page	N/A	N/A
Sign In	Username	Provide the username.
	Password	Provide the password.

Application Action	Action Parameters	Parameter Description
Create a New Sheet	N/A	N/A
Input Data	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Key text 1	Provide the key text.
	Value text 1	Provide the value text
	Key text 2	Provide the key text.
	Value text 2	Provide the value text
	Key text 3	Provide the key text.
	Value text 3	Provide the value text
Share the Sheet	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Receiver username	Provide the username of the receiver.
Complete sharing	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Receiver username	Provide the username of the receiver.
	Sharing note	Provide the text for the sharing note.
Sign Out	Username	Provide the username.
<i>Google Slides</i>		
Load Sigh In Page	N/A	N/A
Sign In	Username	Provide the username.
	Password	Provide the password.
Start a New Presentation	Username	Provide the username.
Start a New Slide	N/A	N/A
Input Slide Text	Slide Name	Provide the value.

Application Action	Action Parameters	Parameter Description
Replace Image	Username	Provide the username.
	File attachment	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Name the Slide	Slide name	Provide the value.
Share the Slide	Username	Provide the username.
	Slide name	Provide the value.
	Receiver username	Provide the username of the receiver.
Send Sharing	Receiver username	Provide the username of the receiver.
Sign Out	Username	Provide the username.
<i>GoogleHangouts</i>		
Load First Page	N/A	N/A
Sign In	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Password	Provide the password.
	Other user's first/last name	Provide the other user's first/last name.
Start Chat	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
Send Text Message	First chat text message	Provide the text message.

Application Action	Action Parameters	Parameter Description
Receive Text Message	N/A	N/A
Send a File	User email address	Provide the user email address.
	Second chat text message	Provide the text message.
Receive Text Reply	User email address	Provide the user email address.
Send Image	N/A	N/A
Receive Image	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
	First chat text message	Provide the text message.
	Second chat text message	Provide the text message.
Make Phone Call	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Phone number	Provide the phone number.
Start Video Call	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
Logout	User's first/last name	Provide the user's first/last name.

Application Action	Action Parameters	Parameter Description
	User email address	Provide the user email address.
<i>GooglePhotos</i>		
Load Login Page	N/A	N/A
Login to Google	Password	Provide the password.
	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
View a Photo	User email address	Provide the user email address.
	Full user name	Provide the username.
View Next Photo	Full user name	Provide the username.
Return to Main Page	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
View Albums Page	Shared folder name	Provide the folder name.
Select an Album	User email address	Provide the user email address.
	Full user name	Provide the username.
	Shared folder name	Provide the folder name.
Upload a Photo	Uploaded Photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to

Application Action	Action Parameters	Parameter Description
		upload a file.
Return to Photos Page	N/A	N/A
Download a Photo	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout of Google	User email address	Provide the user email address.
	Full user name	Provide the username.
<i>HTTP</i>		

Application Action	Action Parameters	Parameter Description
HTTP GET	Path	The value of the path requested.
	Query	The value of the query requested.
	Request headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Accept-Language • Sec-Fetch-User • Upgrade-Insecure-Requests • Sec-Fetch-Site <p>Use the Add button to add new options or the Delete to remove them.</p>
	Status code	The value of the response status code.
	Reason phrase	The value of the reason phrase.
	Response headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Cache-Control • Etag <p>Use the Add button to add new options or the Delete to remove them.</p>
	Response body	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file. • Dynamic payload - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
HTTP POST	URL	Provide the URL.
	Request headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Sec-Fetch-User • Upgrade-Insecure-Requests • Accept-Language • Sec-Fetch-Site <p>Use the Add button to add new options or the Delete to remove them.</p>
	Request body	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file. • Dynamic payload - select an option from the drop-down list or use the Upload button to upload a file.
	Status code	The value of the response status code.
	Reason phrase	The value of the reason phrase.
	Response headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Etag • Cache-Control <p>Use the Add button to add new options or the Delete to remove them.</p>
	Response Body	Add a response message.
<i>Jingdong</i>		
Go To Jingdong	N/A	N/A
Login	Username	Provide the username.
Search For products	Search keyword	Provide the search criteria.
Check Products Information	N/A	N/A

Application Action	Action Parameters	Parameter Description
Checkout	Username	Provide the username.
	Product name	Provide the product name.
	Order ID	Provide the order ID.
Logout	N/A	N/A
<i>Jira</i>		
Load Login Page	Story name	Provide the story name.
Login	Login email address	Provide the login email address.
	Password	Provide the password.
Create Project	Login email address	Provide the login email address.
	Project name	Provide the project name.
Create Story	Project name	Provide the project name.
	Story name	Provide the story name.
Add Comments to Story	Story name	Provide the story name.
Mark The Story To Closed	Story name	Provide the story name.
Logout	Story name	Provide the story name.
<i>League of Legends</i>		
Login	User ID	Provide the user ID.
Start Game	User ID	Provide the user ID.
Attack	N/A	N/A
<i>Mail.ru</i>		
Login	Username	Provide the username.
	Password	Provide the password.

Application Action	Action Parameters	Parameter Description
Send Mail	Fullscreen	Provide the fullname.
	Recipient email address	Provide the recipient email address.
	Recipient email subject	Provide the email subject.
	Recipient email body	Provide the email body.
View Mail	Fullscreen	Provide the fullname.
	Message sender email	Provide the sender email.
	Message sender name	Provide the sender name.
	View message subject	Provide the message subject.
	View message body	Provide the message body.
Logout	N/A	N/A
<i>Meraki</i>		
Login	Dashboard email address	Provide the email address.
	Dashboard password	Provide the password.
Enroll Device	New device address	Provide the device address.
	Enrollment message	Provide an enrollment message.
Add Application	New device address	Provide the device address.
	New application search query	Provide the search criteria.
Add Profile	New device address	Provide the device address.

Application Action	Action Parameters	Parameter Description
	Test profile name	Provide the test profile name.
	Test profile description	Provide the test profile description.
	Backup file name	Provide the backup file name.
Push Updates	N/A	N/A
View Clients	New device address	Provide the device address.
View Map	New device address	Provide the device address.
View Logs	New device address	Provide the device address.
Download CSV	Dashboard email address	Provide the email address.
Send Command	Remote command line	Provide the remote command line,
View Summary	New device address	Provide the device address.
Add Geofence	Geofence name	Provide the geofence name.
	Area name	Provide the area name.
Add Policy	Policy name	Provide the policy name
Add owner	New device address	Provide the device address.
	Owner name	Provide the name.
	Owner username	Provide the username.
	Owner password	Provide the password.
	Owner email	Provide the email.
Logout	N/A	N/A
<i>Mewe</i>		
Open Login Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Login	Email	Provide the email address.
	Password	Provide the password.
Read News Feed	N/A	N/A
Post Status	Status message	Provide the message text.
Logout	N/A	N/A
<i>MongoDB</i>		
Insert	N/A	N/A
Update	N/A	N/A
Query	N/A	N/A
Get More	N/A	N/A
Delete	N/A	N/A
Kill Cursor	N/A	N/A
Diagnostic Messages	N/A	N/A
<i>Netease</i>		
Go to Netease Music	N/A	N/A
Login	N/A	N/A
Search Music	Artist ID	Provide the artist ID.
PlayMusic	Music file name 1	Provide the music file name.
	Music file name 2	Provide the music file name.
	Music file name 3	Provide the music file name.
	Music file name 4	Provide the music file name.
Add To Playlist	Artist ID	Provide the artist ID.
Recommend Music	Artist ID	Provide the artist ID.

Application Action	Action Parameters	Parameter Description
Watch Music Video	Artist ID	Provide the artist ID.
	Music video ID 1	Provide the music video ID.
	Music video ID 2	Provide the music video ID.
	Music video ID 3	Provide the music video ID.
	Music video ID 4	Provide the music video ID.
Logout	N/A	N/A
<i>Office 365 Outlook People</i>		
Get Sign In Page	N/A	N/A
Sign In	User name	Provide the user name.
	Password	Provide the password.
Create a New Contact	Contact first name	Provide the first name.
	Contact last name	Provide the last name.
	Contact email	Provide the email address.
Search for a Contact	Search people	Provide the search criteria.
Delete a Contact	Contact email	Provide the email address.
Sign Out	N/A	N/A
<i>Office365 Excel</i>		
Get Home Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
Get Excel Tab	N/A	N/A
Get Excel Workbook	Workbook name	Provide the workbook name.
Edit Workbook	Content	Provide the content.
Pin Workbook	Workbook name	Provide the workbook name.
Open Workbook In OneDrive	N/A	N/A
Sign Out	N/A	N/A
<i>Office365 OneDrive</i>		
Get Home Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Get OneDrive Tab	N/A	N/A
Delete File	File name	Provide the file name.
Upload File	File name	Provide the file name.
	Upload file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Create Folder	Folder name	Provide the folder name.
Create Excel Workbook	Workbook name	Provide the workbook name.
Create Word	Document name	Provide the document name.

Application Action	Action Parameters	Parameter Description
Document		
Create Powerpoint Presentation	Powerpoint name	Provide the powerpoint name.
Sign Out	N/A	N/A
<i>Office365 Outlook</i>		
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
View Inbox	N/A	N/A
Send Message	Recipient	Provide the email address.
	Subject	Provide the email subject.
	Body	Provide the email body text.
Send Message With Attachment	Recipient	Provide the email address.
	Subject	Provide the email subject.
	Body	Provide the email body text.
	Attachment	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Attachment filename	Provide the file name.
Open Message	N/A	N/A
Delete Message	N/A	N/A

Application Action	Action Parameters	Parameter Description
Navigate To Calendar Panel	N/A	N/A
Create A New Event	Event date	Set the event date.
	Event start time	Set the start time.
	Event end time	Set the end time
	Event name	Set the event name.
Delete An Event	Event date	Set the event date.
	Event start time	Set the start time.
	Event end time	Set the end time
	Event name	Set the event name.
Navigate to People Panel	N/A	N/A
Create a New Contact	Contact email	Provide the address email.
	First name	Provide the first name.
	Second name	Provide the second name.
	Phone number	Provide the phone number.
Search For A Contact	Search string	Provide the search criteria.
Delete A Contact	Contact email	Provide the address email.
	First name	Provide the first name.
	Second name	Provide the second name.
	Phone number	Provide the phone number.
Navigate To Task Panel	N/A	N/A
Create New Task	Task title	Provide the task tile.
Mark Task Completed	Task title	Provide the task tile.
Delete Task	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign Out	N/A	N/A
<i>OK.ru</i>		
Login	Username	Provide the user name.
	Password	Provide the password.
View Feed	N/A	N/A
Post Message	Message	Provide the message text.
Logout	N/A	N/A
<i>Portal</i>		
Login	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Search Image	Search query	Provide the search criteria.
Upload Image	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout	N/A	N/A
<i>Reddit</i>		
Load Main Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign In	Username	Provide the user name.
	Account password	Provide the password.
Access Post	N/A	N/A
Create Comment	Comment content	Provide content for the comment.
Delete Comment	N/A	N/A
Search Posts	Query string	Provide the search criteria.
Subscribe to Subreddit	Subreddit	Provide the subreddit.
Access Gifts Page	Subreddit	Provide the subreddit.
Load Profile	Username	Provide the user name.
Access Settings	N/A	N/A
Access Messages	N/A	N/A
Sign Out	N/A	N/A
<i>Salesforce</i>		
Load Login Page	User name	Provide the user name.
Login	User name	Provide the user name.
	Login email address	Provide the login email address.
	Password	Provide the password.
Select Top Deal	User name	Provide the user name.
	Login email address	Provide the login email address.
Update Call Log	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Opportunities Tab	Login email address	Provide the login email address.

Application Action	Action Parameters	Parameter Description
Select An Opportunity	User name	Provide the user name.
	Login email address	Provide the login email address.
Edit Amount	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Notes Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Edit a Note	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Dashboards Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Opoen Adoption Dashboard	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Calendar Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Add a Meeting	User name	Provide the user name.
	Login email address	Provide the login email address.
Logout	User name	Provide the user name.
	Login email address	Provide the login email address.
<i>Service-Now</i>		
Get Sign In Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign In	Username	Provide the user name.
	Password	Provide the password.
View an Incident	Username	Provide the user name.
	Incident number searched	Provide the incident number.
	Search shot description	Provide a description.
Create an Incident	Username	Provide the user name.
	Incident number searched	Provide the incident number.
	Description	Provide a description.
	Caller	Provide the caller.
	Caller email	Provide the caller email.
Sign Out	N/A	N/A
<i>Skype 8</i>		
Sign In	Sign-in address	Provide the email address.
	Password	Provide the password.
Add Contact	Contact email address	Provide the email address.
	Contact's first/last name	Provide the first/last name.
View Contact Profile	Contact email address	Provide the email address.
Send an IM	N/A	N/A
Receive an IM	N/A	N/A
Start Audio Call	N/A	N/A
End Audio Call	N/A	N/A
Sign Out	N/A	N/A

Application Action	Action Parameters	Parameter Description
<i>Skype</i>		
Login	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
	Peer activity message	Provide the message.
Video Call	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
End Video Call	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
Voice Call	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
End Voice Call	Login email address	Provide the email address.
	User name	Provide the user name.

Application Action	Action Parameters	Parameter Description
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
Logout	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
	Peer activity message	Provide the message.
<i>SMTP</i>		
Ehlo	N/A	N/A
Auth Login	N/A	N/A
Send Mail	Email subject	Provide the email subject.
	Email content	Provide the email content.
	Number of attachment	Provide the value for the number of attachment.
	Attachment Content	Provide the attachment content.
Quit	N/A	N/A
<i>Social Network</i>		
Login	Login username	<p>Select an option:</p> <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	<p>Select an option:</p> <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
		file.
News feed	N/A	N/A
View Profile	Member ID	Provide the member ID.
Like Post	N/A	N/A
Unlike Post	N/A	N/A
Create Post	Post content	Provide the content.
Comment To Post	Original post ID	Provide the post ID.
	Comment content	Provide the content.
Logout	N/A	N/A
<i>Splunk</i>		
Load Login Page	N/A	N/A
Login	Username	Provide the user name.
	Password	Provide the password.
Upload Log	Description	Provide a description.
	Index	Provide the index.
	Log File	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Search Log	Index	Provide the index.
Logout	Username	Provide the user name.
<i>Tubi</i>		
Open Tubi Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Login	Email address	Provide the email address.
	Password	Provide the password.
	User ID	Provide the user ID.
	User name	Provide the user name.
Browse Tubi	Genre	Provide the genre.
Select Movie	Genre	Provide the genre.
	Movie name	Provide the movie name.
	Movie duration	Provide the movie duration.
	Movie description	Provide the movie description.
	Movie director	Provide the movie director.
	Movie release year	Provide the release year.
	Movie actor 1	Provide the movie actor.
	Movie actor 2	Provide the movie actor.
	Movie content ID	Provide the movie content ID.
	Recommended movie name	Provide the recommended movie name.
Play Video	Movie content ID	Provide the movie content ID.
Pause Video	Movie content ID	Provide the movie content ID.
Selet Recommended Movie	Genre	Provide the genre.
	Recommended movie name	Provide the recommended movie name.
	Recommended movie duration	Provide the recommended movie duration.
Logout	N/A	N/A
<i>TWC</i>		
Open The Weather Channel App	N/A	N/A

Application Action	Action Parameters	Parameter Description
View 48 Hours Details	N/A	N/A
View 15 Days Details	N/A	N/A
Swipe to Bottom of Main Page	N/A	N/A
<i>Video Platform</i>		
Login	Login username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Search Video	Video name	Provide the video name.
Download video	Downloaded file name	Provide the file name.
	Downloaded file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Upload Video	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Delete Video	N/A	N/A

Application Action	Action Parameters	Parameter Description
Like Video	N/A	N/A
Unlike Video	N/A	N/A
Logout	N/A	N/A
VKontakte		
Load Login page	N/A	N/A
Login	Username	Provide the user name.
	Password	Provide the password.
View Feed	View feed message	Provide the message.
Post Message	Post message	Provide the message.
Logout	N/A	N/A
Yammer		
Select First Group	User email address	Provide the email address.
	User name	Provide the user name.
Select Second Group	User email address	Provide the email address.
Select Third Group	User email address	Provide the email address.
Like an Entry	User email address	Provide the email address.
Reply to a Post	User email address	Provide the email address.
	User name	Provide the user name.
Post New Message	User email address	Provide the email address.
	User name	Provide the user name.
Select Another Group	User email address	Provide the email address.

Application Action	Action Parameters	Parameter Description
<i>YYLive</i>		
Load Home Page	N/A	N/A
Select Category	Category	Provide the category.
Play Video	Video ID	Provide the Video ID.

The difference between Dynamic and Payload files

- If the chosen file is Payload (not Dynamic), the exact contents of the file can be seen on the wire.
- If the chosen file is Dynamic and the file does not contain Macros, then the behavior is the same as above.
- If the chosen file is Dynamic and the file contains Macros, then each Macro is evaluated during the test with the expected value that the Macro is meant to generate.

Artifacts

This section contains useful information and details on Playlist and Macro features.

Rules and Grammar for Playlists

Rules to support comma or double-quotes as a part of a playlist:

1. Each playlist item with comma or double-quote in the content **must** be enclosed within double-quotes.
2. Every double-quote used as a part of the content must be escaped with another double-quote.

Each record is located on a separate line, delimited by a line break (CRLF). For example: `record = value * (COMMA value)` :

Record	value 1	value 2
abcd	abcd	
abcd,wxyz	abcd	wxyz
"abcd,pqr","wxyz"	abcd,pqr	wxyz
"abcd,pq""r","wxyz"	abcd,pq"r	wxyz

For all applications that have a **Sign In** or **Sign Up** action, the following parameters offer the possibility of uploading a playlist file: Login Username, Login password or SignUp Username, SignUp password, SignUp confirm password. Select the **Playlist file** option and select the **Upload** option:

The screenshot shows the 'Traffic Profiles (1 application)' configuration screen. On the left, under 'Traffic Profile Configuration', there's a sidebar with 'Predefined Applications' and a section for 'Applications' which lists 'eBanking Chrome to Apache 1'. The main area has two tabs: 'Actions' and 'Properties'. The 'Actions' tab displays a list of actions with columns for '#', 'Name', and 'Weight'. The 'Properties' tab shows fields for 'Login username' (set to 'Playlist file'), 'Login password' (set to 'User input' with value 'user1pass'), and an 'Upload' button highlighted with a red circle.

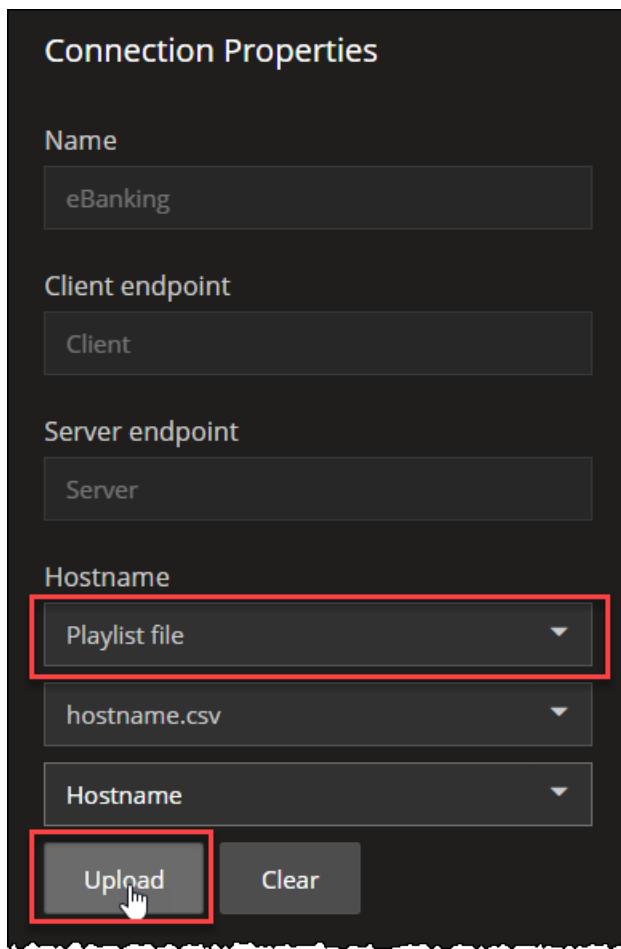
After the upload is performed, the reference column has corresponding csv column names, which can be chosen from the dropdown menu:

This screenshot shows the same interface after a CSV file has been uploaded. In the 'Properties' section, the 'Username' field now contains 'Username' and is highlighted with a red box, indicating it is the selected reference column. The other fields ('Password' and 'Login password') remain set to 'User input' and 'user1pass' respectively.

For some applications, the Hostname (under **ConnectionProperties**) offers the possibility of uploading a playlist file:

1. Select the **Playlist** file option .
2. Select **Upload**.

3. Choose the **Reference** column name from the drop-down.



Example of a Hostname playlist file:

NOTE As of now, we do not validate empty Hostname values, if they are fetched from a playlist file.

	A	B
1	Hostname	
2	server1.com	
3	server2.com	
4	server3.com	
5	server4.com	
6	server5.com	
7	server6.com	
8	server7.com	
9	server8.com	
10	server9.com	
11	server10.com	
12		
13		
14		
15		
16		
17		

hostname(4107)

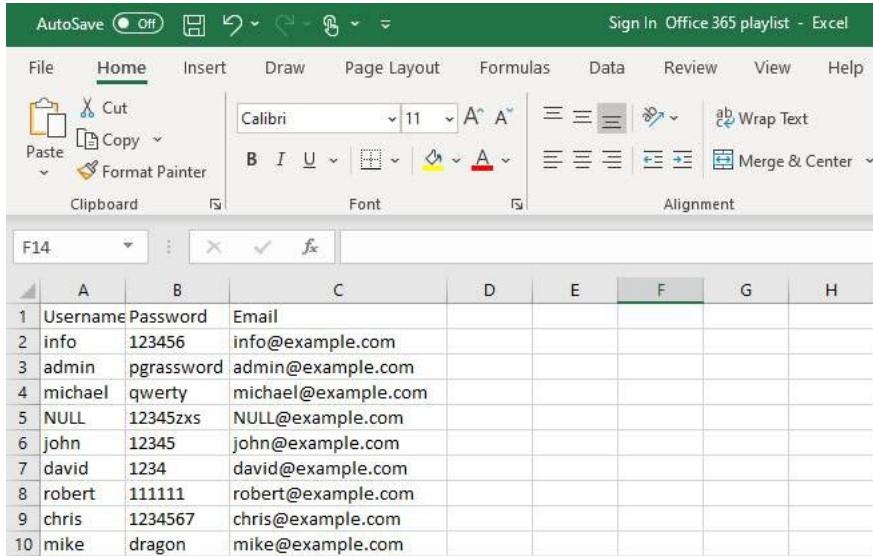
About Playlists

For the **Sign In** action in eBanking, eShop, Social Network, Portal or the **Sign Up** action in eBanking applications, please use this [Sign In playlist](#) file:

Sign In playlist - Excel

	A	B	C	D	E	F	G	H	I
1	Username	Password							
2	admin	pgrassword							
3	michael	qwerty							
4	NULL	123456789							
5	john	12345							

For the **Sign In** action in Office 365 (Outlook, Excel, OneDrive) applications , please use this [Sign In Office 365 playlist](#) file:



The screenshot shows a Microsoft Excel spreadsheet titled "Sign In Office 365 playlist - Excel". The table contains 10 rows of data with columns labeled A through H. Column A is "Username", column B is "Password", and column C is "Email". The data is as follows:

	Username	Password	Email				
1	info	123456	info@example.com				
2	admin	pgrassword	admin@example.com				
3	michael	qwerty	michael@example.com				
4	NULL	12345zxs	NULL@example.com				
5	john	12345	john@example.com				
6	david	1234	david@example.com				
7	robert	111111	robert@example.com				
8	chris	1234567	chris@example.com				
9	mike	dragon	mike@example.com				
10							

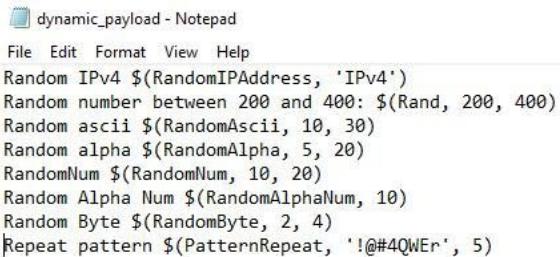
About Macros

A macro is a method or function which allows you to customize the payload text data with the following parameters. The `maxLength` limit is set to 1024:

Macros	Description
<code>\$(RandomIPAddress, 'IPv4')</code>	The RandomIPAddress macro randomly generates IPv4 address. IPv6 is not yet supported.
<code>\$(Rand, minValue, maxValue)</code>	The Rand macro generates one random number within the range [minValue, maxValue]. It takes one or two parameters. Range is 0 – N or N1 – N2.
<code>\$(RandomAscii, minLength, maxLength)</code>	The RandomAscii macro generates a sequence of random Ascii characters with values in the range: 0-127 minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomAlpha, minLength, maxLength)</code>	The RandomAlpha macro generates a sequence of random letters [A-Za-z]. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomNum, minLength, maxLength)</code>	The RandomNum macro generates a sequence of random digits minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomAlphaNum, minLength, maxLength)</code>	The RandomAlphaNum macro generates a sequence of random letters or digits [A-Za-z0-9]. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.

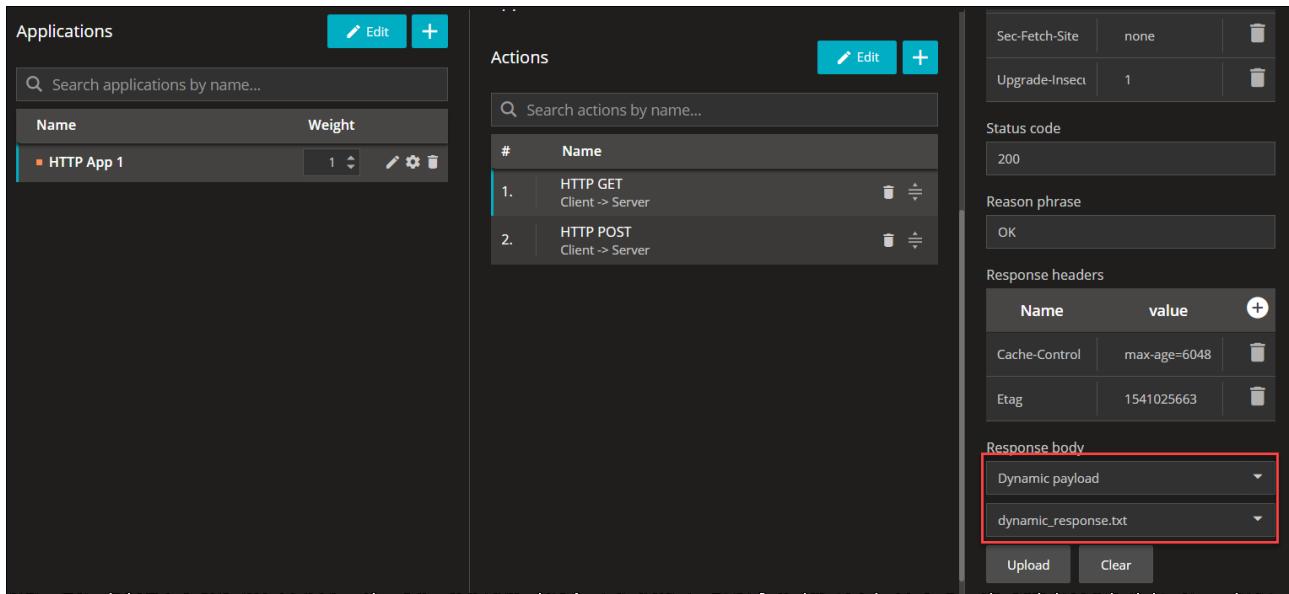
\$(RandomByte, minLength, maxLength)	The RandomByte macro generates a sequence of random bytes. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
\$(PatternRepeat, pattern, minLength, maxLength)	The PatternRepeat macro generates a sequence of characters by repeating the <pattern> pattern. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length. If the chosen length is not an exact multiple of the length of <pattern>, the last repetition of <pattern> is truncated.

The following is the macro file structure, and please use this [macros](#) file for the correct file format:



```
dynamic_payload - Notepad
File Edit Format View Help
Random IPv4 $(RandomIPAddress, 'IPv4')
Random number between 200 and 400: $(Rand, 200, 400)
Random ascii $(RandomAscii, 10, 30)
Random alpha $(RandomAlpha, 5, 20)
RandomNum $(RandomNum, 10, 20)
Random Alpha Num $(RandomAlphaNum, 10)
Random Byte $(RandomByte, 2, 4)
Repeat pattern $(PatternRepeat, '!@#4QWEr', 5)
```

This feature is also available for the HTTP application, on both HTTP GET and HTTP POST actions, under the following parameters: Response body/Response body. Switch to the dynamic payload and upload the `dynamic_payload` file:



The screenshot shows the ZAP interface with the following details:

- Applications:** Shows a single application named "HTTP App 1" with a weight of 1.
- Actions:** Shows two actions:
 - Action 1: HTTP GET Client -> Server
 - Action 2: HTTP POST Client -> Server
- Response headers:** Includes fields for Sec-Fetch-Site (none), Upgrade-Insecure (1), Status code (200), Reason phrase (OK), Cache-Control (max-age=6048), and Etag (1541025663).
- Response body:** This section is highlighted with a red box. It contains two dropdown menus:
 - Top dropdown: Dynamic payload
 - Bottom dropdown: dynamic_response.txt

Assign the agents, enable capture and start the test. After the test is finished, download the captured information and you can see the payload, as set in the macro file:

Appendix B Cu IsolationApplication Actions

Apply a display filter <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
16	0.099346	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 48737 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983045 TSecr=807789105
17	0.099359	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 37775 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983119 TSecr=807784865
18	0.099366	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 58394 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983026 TSecr=807847657
19	0.099374	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
20	0.099378	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
21	0.099378	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
22	0.099623	192.168.10.90	192.168.10.91	HTTP	590	HTTP/1.1 200 OK (text/plain)
23	0.099624	192.168.10.90	192.168.10.91	HTTP	602	HTTP/1.1 200 OK (text/plain)
24	0.099646	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 36116 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983171 TSecr=807846794
25	0.099651	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
26	0.099685	192.168.10.90	192.168.10.91	HTTP	582	HTTP/1.1 200 OK (text/plain)

```

> Frame 22: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: VMware_A6:29:b9 (00:0c:29:a6:29:b9), Dst: VMware_99:5a:02 (00:0c:29:99:5a:02)
> Internet Protocol Version 4, Src: 192.168.10.90, Dst: 192.168.10.91
> Transmission Control Protocol, Src Port: 80, Dst Port: 58394, Seq: 1, Ack: 306, Len: 524
> Hypertext Transfer Protocol
Line-based text data: text/plain (12 lines)
Random IPv4 158.243.103.228\r\n
Random number between 200 and 400: 266\r\n
Random ascii \016\035EY\023Te1.'\]:\034+/?\031p*\026qI\030\024<\r\n
Random alpha VEKzKn\r\n
RandomNum 227499253664034\r\n
Random Alpha Num RDtTu0@LmL\r\n
Random Byte Y♦\r\n
Repeat pattern !@#4QWEr!@#4QWEr!@#4QWEr!@#4QWEr!\r\n
\r\n
\r\n
\r\n
\r\n

```

Index

A

Access Control 388
 administrator
 change password 16
 initial login 16
 Agent Management, accessing 388
 agents

 clear ownership 80
 management 78
 Network Management window 81
 ownership 76
 reboot 80
 status of 78
 tags 79
 application traffic generator 216, 274, 301, 304, 322

B

bidirectional UDP traffic flow 278

C

create/delete PDU session, secondary objective 269
 create/delete QoS Flows, secondary objective 266
 customer assistance 3

D

DNN settings
 Full Core tests 55

E

enter/exit idle, secondary objective 266

F

Full Core tests
 network slicing 254

I

inter-CU handovers 87

J

jumbo frames 53

L

License Manager, accessing 388

N

Network Management window 81

P

Paging, secondary objective 265
 passthrough interface 129
 passwords

 admin, change 16
 user, change 19

product support 3

Q

QoS flows, settings 63

S

SMS, secondary objective 270
 software updates 388
 stateless UDP traffic generator 192, 272
 statistics
 licensing stats 383
 view in real time 41

System Monitor 388

T

tags

 custom 79

 types 75

technical support 3, 388

traffic generators 190, 271

U

UDP stateless, traffic generator 192, 272

updates 388

user

 accounts 385

 management 388

 preferences 388



This information is subject to change
without notice.

www.keysight.com