Keysight Open RAN Simulators, Cloud Edition 3.1

CuSIM

User Guide

KEYSIGHT

Notices

Copyright Notice

Warranty

Technology Licenses

U.S. Government Rights

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
Regional and local support contacts:		
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

CHAPTER 1
CuSIM 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 CuSIM is a cloud-native gNB Central Unit (CU) simulator that provides comprehensive support for testing the performance and functionality of your gNB Distributed Units (DUs) in a standalone (SA) network topology. It simulates user plane and control plane traffic flowing over the F1 interface from a simulated gNB-CU to your gNB-DU (the DUT), and it responds to traffic sent from your DUT to the simulated gNB-CU.

CuSIM also includes basic 5G-Core functionality to handle NAS Layer procedures without a 5G-Core simulation tool.

Chapter contents:

CuSIM feature summary

CuSIM 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).

CuSIM feature summary:

- Supports testing in 5G SA networks.
- Features a web-based user interface (UI) through which you manage all aspects of your CuSIM testing environment, including test creation, execution, and management; traffic agent deployment and management; statistical results and reporting; and user and license administrative control.
- Traffic agents generate traffic over the F1-U (user plane) and F1-C (control plane) interfaces. The agents are implemented as containers or virtual machines, depending upon the platform on which they are deployed. The supported platforms include:
  - 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 CuSIM 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 the facing page](#)
- [Statistics page on page 11](#)

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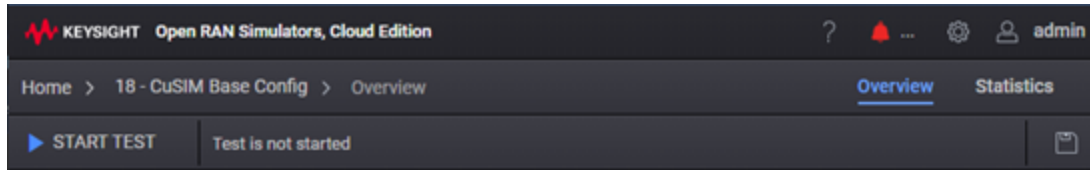
In addition to the information in this topic, refer to these topics for more information about the available tools and functions:

- [CuSIM title bar settings on page 180](#)
- [Save test sessions on page 163](#)

Test Overview page

When you open or create a test session based on any predefined, newly-created, or imported test configuration, CuSIM 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.
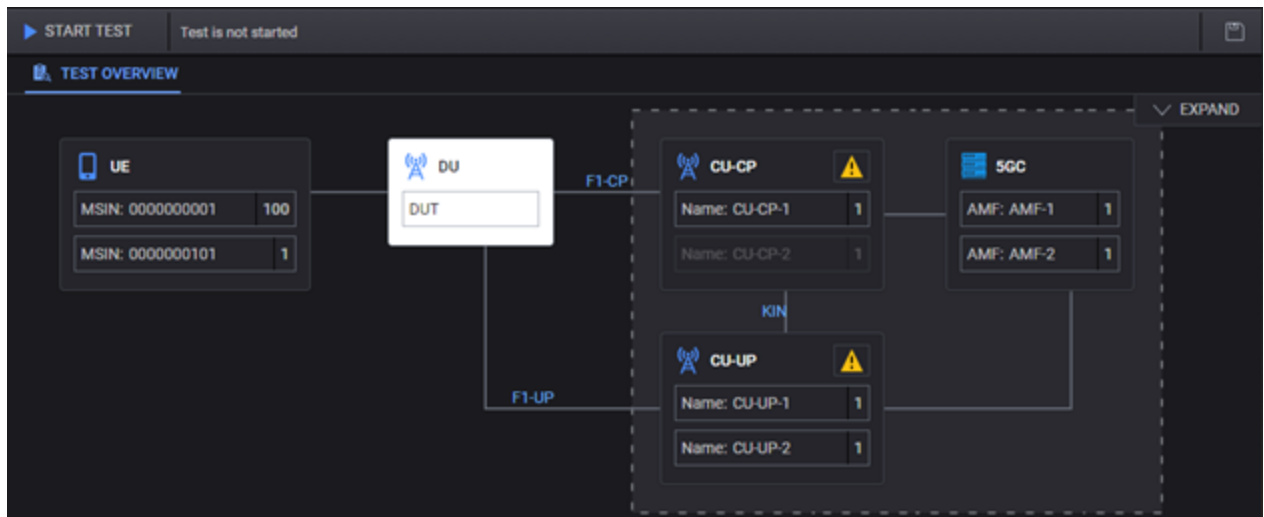
The test topology is an interactive graphical representation of the test network. From the topology, you access all of the configurable elements for the current test. These include the DUT (your gNB-DU), the CU (which is represented as a CU-CP node and a CU-UP node), the 5G core, and the user endpoints (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 F1 procedure rates, RRC procedure rates, NAS procedure rates, user plane throughput rates, 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 CuSIM 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 14](#)

Required information

- The IP address that you set for the CuSIM 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 CuSIM license activation codes (or entitlement codes).

Initial login and password change

CuSIM 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 CuSIM instance in your browser's address field.
   CuSIM 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, CuSIM 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 .0 title bar.
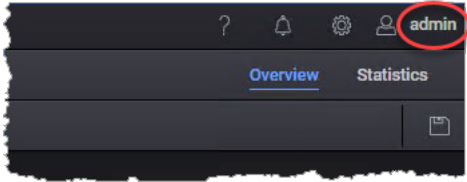
Keysight Open RAN Simulators, Cloud Edition .0 opens the **Edit Account** page in a new browser tab.

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 CuSIM deployment.

To activate your licenses:

1. Select **Administration** from the setup menu (⚙).

2. Select **License Manager** from the **Adminstration** menu. CuSIM opens the **License Manager** page.

3. To activate your licenses:

    a. Select **Activate licenses**.

        CuSIM 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 (⚙).
    CuSIM 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 for detailed information about user account management.

CHAPTER 3
User login and logout

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

Log in as a regular user

The user accounts that the CuSIM 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 CuSIM 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 .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, CuSIM opens the dashboard.

Log out

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

CHAPTER 4
Build and run a test

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

Chapter contents:

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 CuSIM.

2. In the Dashboard page, select the **Wireless CuSIM** template from the **Create New Test** panel. For example:
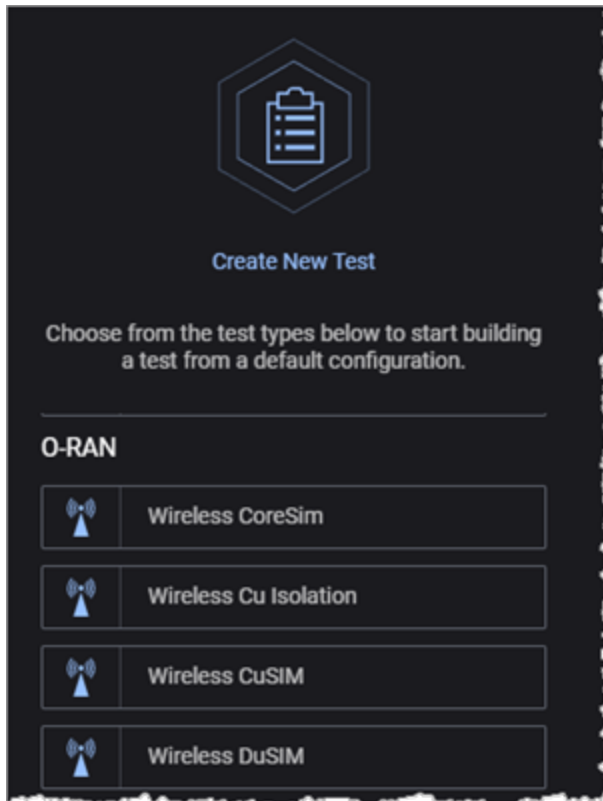
CuSIM opens the **Test Overview** page, which includes the graphical representation of the test topology. By default, SA topology is activated. You need to select NSA or CU-Simulated node for another network topology.

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

3. Assign a name to your new test config:

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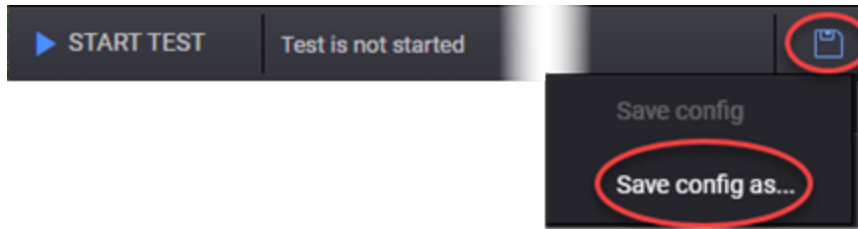
    CuSIM opens the **Save config as** dialog.

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

The new test config is immediately available.

> **NOTE**
>
> The terms *test config* and *test session* are not entirely synonymous. A "config" refers to a configuration definition file (JSON format), whereas a "session" is an instance of that file that is loaded in memory and is capable of being run. Refer to Manage and use test sessions on page 162 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 CuSIM 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 .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** wndow.

2. Click **Expand** if the Test Overview section is collapsed.

3. Click the **Edit** button on the Global Settings section to open the **Global Settings** panel.

   ✎

4. Configure the settings that you will need in your test.

   Many of these settings are important for the proper execution of your tests and for establishing the parameters that control logging, captures, and statistics collection.

Refer to for a description of all of the settings.

Step 3: Configure CU-CP test nodes

The CuSIM 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.

   CuSIM 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:
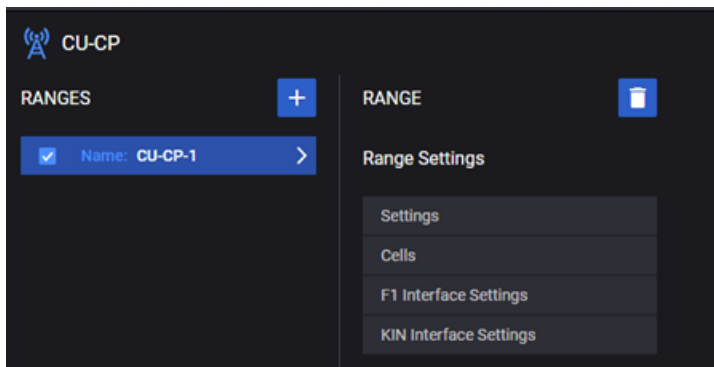
3. Configure each of the settings, which are described in gNB CU-CP configuration settings on page 44.

Step 4: Configure CU-UP test nodes

The CuSIM 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
CuSIM manages DU-UP ranges as follows:

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

- If you delete a DU-CP range, CuSIM 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, CuSIM does not deselect the corresponding DU-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.
   CuSIM 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:
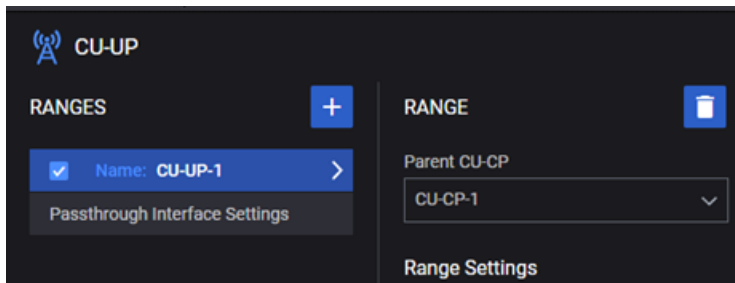
3. Configure each of the settings, which are described in CU-UP Range settings on page 56.

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 59.

Step 5: Configure 5G Core Settings

The CuSIM test topology includes a representation of the simulated 5G Core/AMF information in your test configuration.

1. Select AMF from the topology window. CuSIM opens the 5GC AMF RANGES panel.

2. Select the name of a range (such as AMF-1) to access the configuration settings. For example:
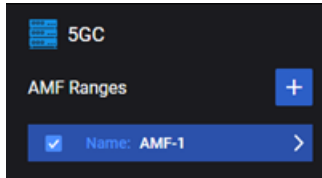
3. Configure each of the settings, which are described in AMF Range panel on page 63.

Step 6: Assign agents to the CU test nodes

You cannot run a CuSIM 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.

   CuSIM 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
	will be one of the following: • 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	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).
Tags	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 36 for more information about tags.
Connections	The table displays the available interface and the MAC address for each wireless connection. The interface can be selected from the drop-down list. NOTE For the CuSIM nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.

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

See also, Assign and manage agents on page 35.

Step 7: Configure UEs

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

1. Select **UE** from the CuSIM topology window.

    CuSIM 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.)

    CuSIM 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. Configure the detailed settings, which include Identity settings and Security Settings of the range. See UE configuration settings on page 65 for detailed descriptions.

    c. Configure **Objectives** for the range:

        i. In the **RANGE** panel, in the **Objectives** section, select **Control Plane**. Configure Test Duration per UE range. If there are multiple UE ranges in a test, it will be stopped based on the maximum specified duration value.

        ii. In the **RANGE** panel, in the **Objectives** section, select **User Plane**. CuSIM opens the **User Plane** panel.

        iii. Add each **Application Traffic** type that you need for the UE range. See UE Test Objective settings on page 76 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.

        CuSIM opens that UE **RANGE** panel.

    b. Click the **Delete Range** button. CuSIM deletes the range from your test config.

Step 8: Start the test
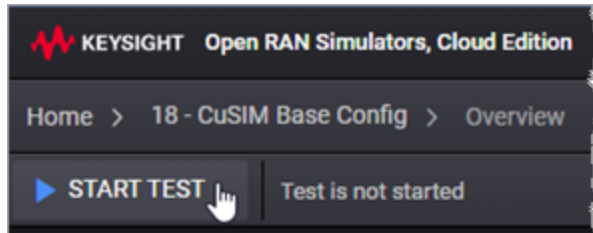
Once you have configured all the properties needed for your test, click the **START TEST** button.

Once you start a test, the CuSIM tool bar displays the test status throughout its execution progress. In addition, each test session tile (located on the CuSIM 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.

CuSIM 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, CuSIM 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. CuSIM 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 9: View real-time test results

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

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

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

Statistics page

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

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

Statistics groupings

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

Overview statistics include:

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

Application Traffic statistics include:

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

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

Statistics page example
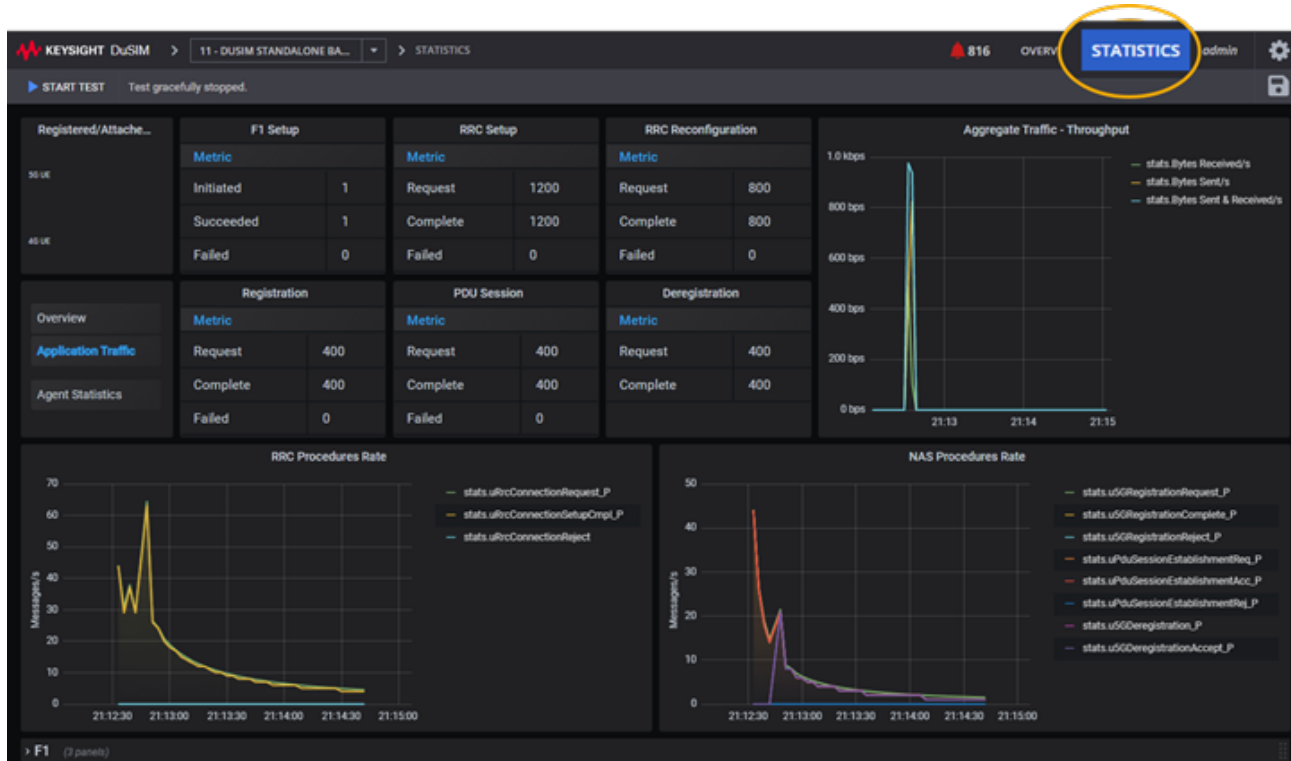
CHAPTER 5
Global Settings

The Global Settings are a list of parameters that have overall applicability to CuSIM 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

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.
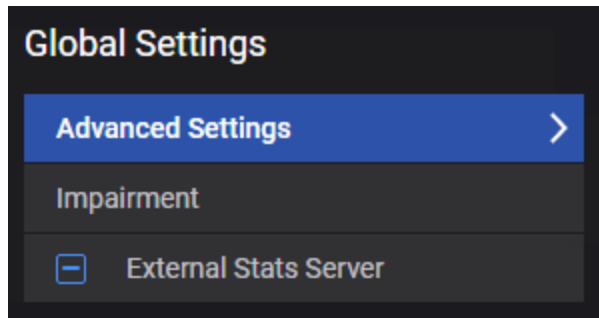
Advanced Settings

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

- [Advanced Settings below](#)
- [Logging Settings on the next page](#)
- [Traffic Settings on page 34](#)

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 *Overwrite Capture Size* 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: • **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 *Automated Polling Interval* option is disabled. It allows you to set a custom polling interval.

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	Select one of the options: • **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	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. Select one or more tags from the drop-down list.

GTPU:

Setting	Description
Log level	Select one of the options: • **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	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. Select one or more components from the drop-down list.
Log Frame Components	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.

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

Control Plane PDCP:

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

User Plane PDCP:

Setting	Description
Log level	Select one of the options: • **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	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

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

Traffic Settings

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

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

External Stats Server

The CuSIM global settings provide an option to designate an external statistics server for testing. To use this feature, specify the server IP address:
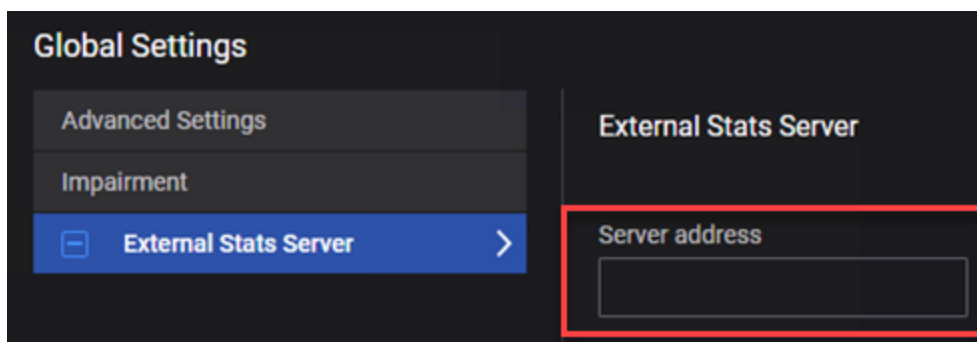
CHAPTER 6
Assign and manage agents

A CuSIM *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

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

Agent implementation

For CuSIM, agents are implemented as VMware ESXi 6.5 and ESXi 6.7 virtual machines in private clouds.

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 CuSIM. 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 39 for instructions.

Assigning agents to nodes

You cannot run a CuSIM 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.

   CuSIM 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
	will be one of the following: • 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	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).
Tags	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 36 for more information about tags.
Connections	The table displays the available interface and the MAC address for each wireless connection. The interface can be selected from the drop-down list. NOTE For the CuSIM nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.

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 CuSIM 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 41](#)

Agent Management window

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

Column	Description
☐	The first column in the table contains a checkbox that you use when selecting individual agents for various operations. Note that you can use the *Agent IP* checkbox in the table header to select all agents.
Agent IP	Displays the IP address of the agent. To see the Agent ID, hover over the agent's IP IP address.
Owner	Indicates whether the agent is assigned, available, or offline.
Status	Indicates the current status of the agent.
Tags	This column displays the tags associated to each agent. There are two types of tags: • system tags (blue): these are defined by CuSIM. 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. Each tag indicates the number of agents to which it was associated.
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	Use this option to filter the available agents by tag names: 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 Agent Management window is updated with the filtering results. To remove the filtering results, select **Clear**.
Include offline agents	Set this option to either include or exclude offline agents from the list.
Search	Search by IP, Owner, hostname, or status.

Adding and removing tags

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

Add a custom tag:

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

Remove a tag:

1. Select one or more agents in the table.

2. Select **Tag as**.

3. Select **Remove tags**.

4. Use the search functionality to identify the tag name or select it from the list.

5. Select **Update** to remove the tag name.

Agent management actions

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

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

Network Management

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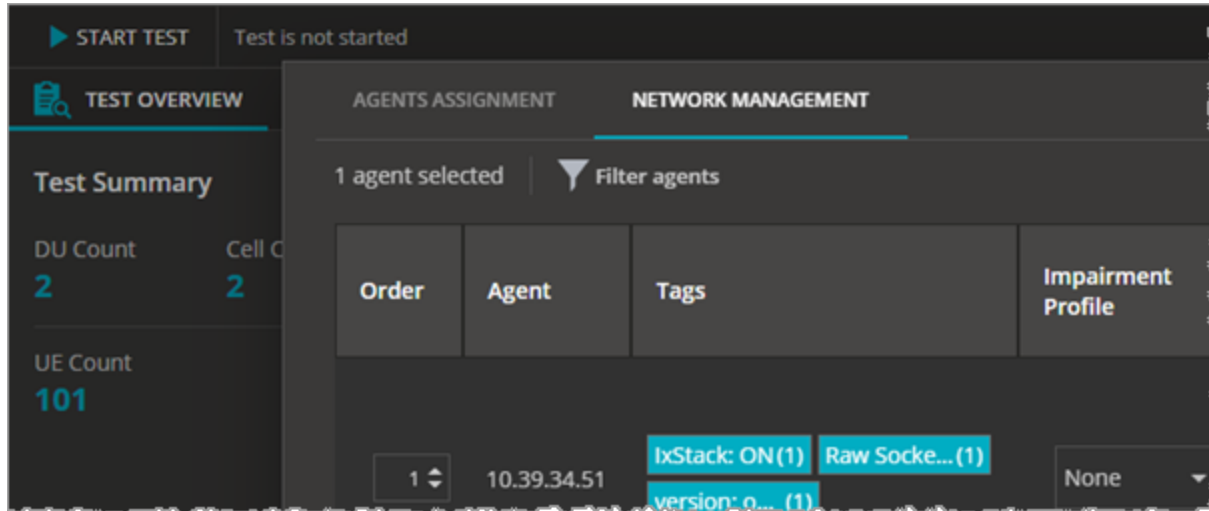
Table description

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

Column	Description
Order	This option allows you to select the agent distribution order when running with multiple agents on the same node (when you are not using a switch to connect all agents).
Agent	Displays the agent's IP address. When hovering over the IP address of the agent, the agent ID is displayed.
Tags	This column displays the tags associated to each agent. There are two types of tags: • system tags (blue): these are defined by CuSIM. 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 40 for more details. Each tag indicates the number of agents to which it was associated.
Impairment profile	Allows you the select an impairment profile from the drop-down list.
Agent Interface	Displays the agent's interface Name and MAC address.

Column	Description
Network Stack	This option allows you to select the network stack used to run the test: • **Linux Stack** • **IxStack over Raw Sockets** • **IxStack over DPDK** An agent compatible with IxStack is marked using an `IxStack: On/Off` system tag.
SRIoV	This option is disabled when *Network Stack* 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 an 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 the 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 (uing tag names) to determine which agents are displayed in the table:

1. Select **Filter agents**.

2. Enter the name of the tag or select it from the available list.

3. Select **Close**.

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

CHAPTER 7

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.
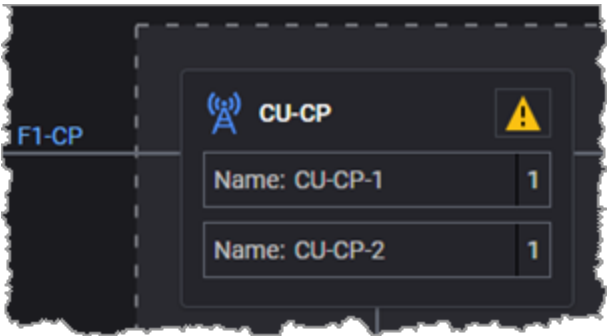
In the CuSIM test topology, the gNB-CU is logically structured as two entities:

- 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 DU is the device under test (DUT) in a Keysight CuSIM test configuration.

Chapter contents:

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 on the facing page 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.
Associated AMF	Select a previously-configured AMF to associate with this CU-CP range.
Range Settings:	
Settings	Each CU-CP range requires the configuration of an associated of Node Settings which are described in section Settings panel on the next page.
Cells	Each CU-CP range requires the configuration of an associated Cells which are described in section Cells settings on page 49.
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 on page 52.
KIN Interface Settings	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 on page 58.

Settings panel

The Settings panel provides access the 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 CuSIM, 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 facing page below.
SCTP Buffers	Refer to SCTP Buffers on the facing page below.
UDP Buffers	Refer to UDP Buffers on the facing 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.
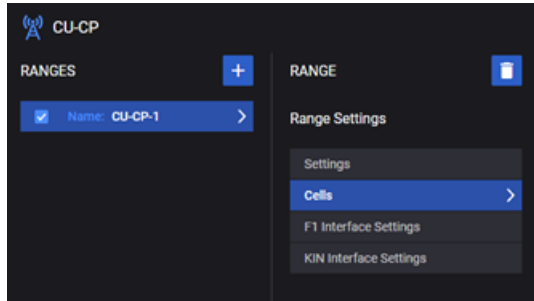
These settings are organized in the following groups:

- 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.
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 2μ x 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.

Settings	Description
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: • 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 next page below.

NSSAI

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

Setting	Description
+	The following actions are available: • 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.
NSSAI panel:	
🗑	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: **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.

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
IP settings:	
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.
VLAN settings:	
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, CuSIM 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**.

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.
Gateway Address	KIN Interface's gateway address.

CHAPTER 8
gNB CU-UP configuration settings

In the CuSIM 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

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:
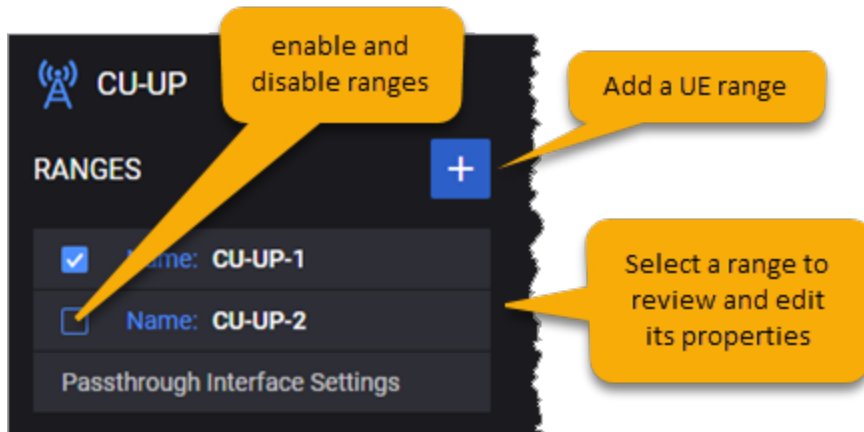
Refer to CU-UP Range settings on the facing page for a description of the CU-UP configuration settings.

CU-UP Range settings

When you select a CU-UP range from the **CU-UP Ranges** panel, CuSIM 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.
Parent CU-CP	Select the parent CU-CP range.
Range Settings:	
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-UP settings on the next page.
KIN Interface Settings	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 on page 58.

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 Interface Settings

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

Setting	Description
F1 Port	The port to use for the F1 connection. The CuSIM 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
IP settings:	
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.
MAC settings:	
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.

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

Setting	Description
IP settings:	
IP Address	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.
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 CuSIM with external traffic servers. When Passthrough Interface is configured, CuSIM traffic configurations do not apply; instead, all traffic is routed to external servers through the configured passthrough interface.

Pasthrough test requirements

The main requirements for CuSIM passthrough test include:

*   Assigning agents to the CU-UP Passthrough Devices, on the Agents Assignment window. For example:
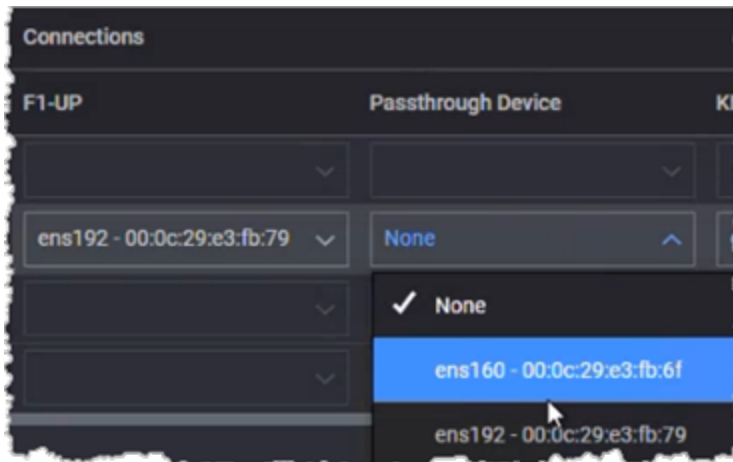
    Refer to Assign and manage agents on page 35 for more information.
*   Configuring at least one L7 server in the Wireless IP Endpoints topology, which is one of the ORAN SIM CE Core topologies (refer to Wireless IP Endpoints on page 86 for detailed information). Note that the Wireless IP Endpoints IP Client node is not required for CU-UP passthrough testing.
*   Configuring a Passthrough Interface at the CU-UP node, as described below.
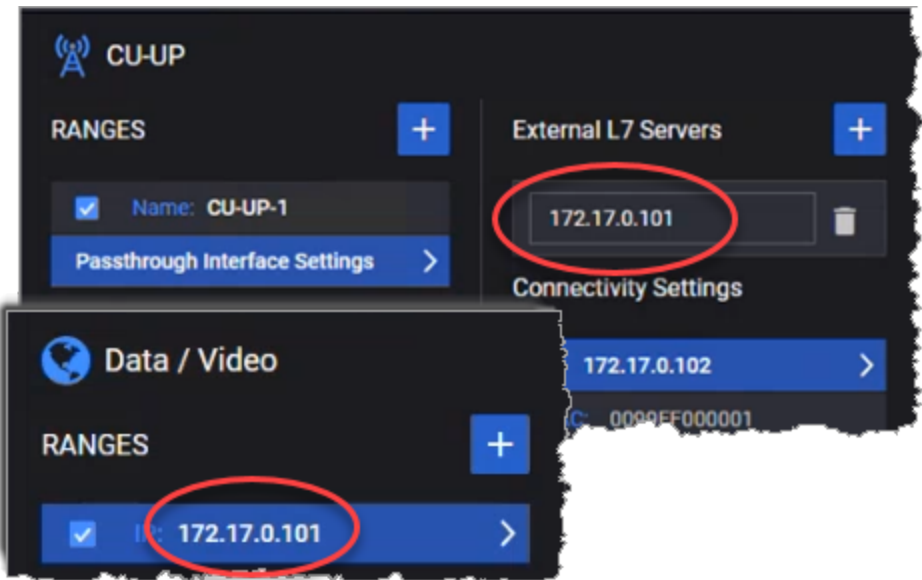
Passthrough interface settings

Select **Passthrough Interface Settings** from the CU-UP Ranges panel.
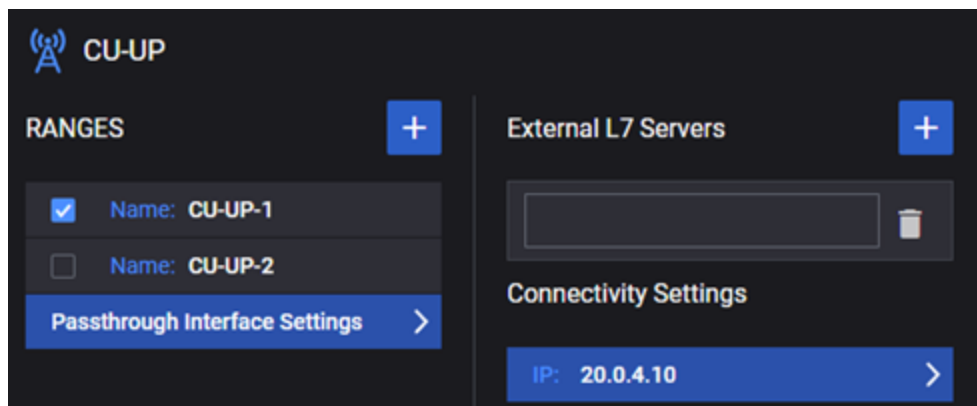
The passthrough interface—when configured—waits for an external traffic source. The following settings are required for the passthrough interface configuration.

Setting	Description
External L7 Servers:	
+	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 intered into the field:
🗑	Delete an External L7 Server entry.
Connectivity settings:	
IP Address	The IP address assigned as the external L7 Server's *Gateway Address* (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.
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.

Setting	Description
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.

CHAPTER 9
5G-Core and AMF configuration settings

CuSIM simulates 5G Core functionality in your tests. You use AMF Ranges to configure the required 5G Core related information.

The AMF Ranges panel opens when you select the AMF node from the network topology window.

Chapter contents:

5GC Ranges panel

The **5GC RANGES** panel opens when you select the 5GC node from the network topology window. You can perform the following tasks from this panel:

- Add AMF ranges.
- Open an AMF range configuration for editing or viewing.
- Enable or disable a range for the test configuration.

For example:

Refer to AMF Range panel below for a description of the range settings.

AMF Range panel

You use AMF Range Panel to configure AMF and 5G Core information.

Parameter	Description
Name	The name uniquely identifies each AMF instance. You can accept the value provided by CuSIM or overwrite it with your own value.
PLMN MCC	The PLMN MCC for this AMF range
PLMN MNC	The PLMN MNC for this AMF range.
Region ID	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.
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. An AMF Region consists of one or multiple AMF Sets. 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).

Parameter	Description
Pointer	The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.
Home Network Private Key	The home network public key that will be used for concealing the Subscription Permanent Identifier (SUPI).
Ciphering Algorithm	Allows to select the supported 5G ciphering algorithm: • NEA0 - Null ciphering algorithm • NEA1 - 128-bit SNOW 3G based algorithm • NEA2 - 128-bit AES based algorithm
Integrity Algorithm	Allows to select the supported 5G integrity protection algorithm: • NIA0 - Null Integrity Protection algorithm • NIA1 - 128-bit SNOW 3G based algorithm • NIA2 - 128-bit AES based algorithm

Mapping CU-CP nodes to AMF ranges

You can create multipe AMF ranges in a CuSIM test, and then map CU-CP ranges to those AMF ranges. For example:
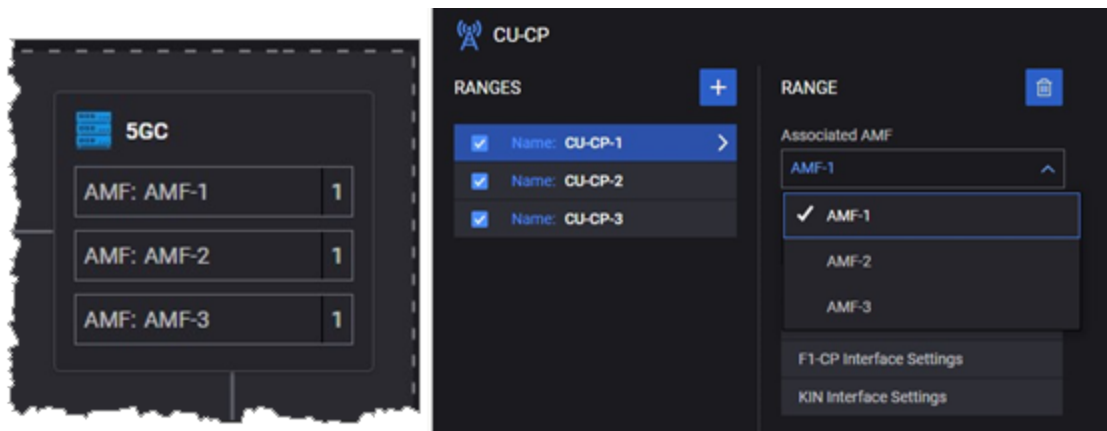
In this example, the CU-CP-1 node is mapped to the AMF-1 range.

CHAPTER 10
UE configuration settings

When you select the **UE** object from the topology window, CuSIM opens the top-level (leftmost) UE properties window.
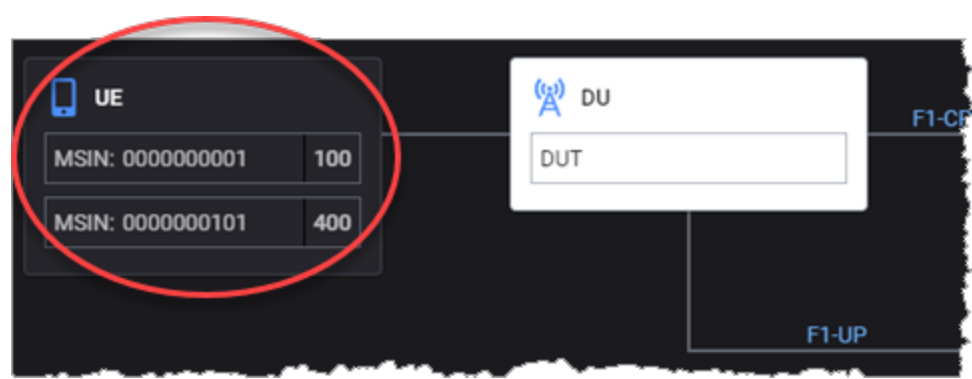
The UE properties include all of the settings required to simulate large and varied groups of subscribers who are attempting to access the test network, establish connections to data networks, transmit (and receive) data of various types, and travel amongst the cells contained within your test network.

The topics in this chapter describe the configuration settings. For procedural instructions, refer to .

Chapter contents:

UE Ranges 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 UEs for your test.

Refer to UE RANGE settings below for a description of the UE configuration settings.

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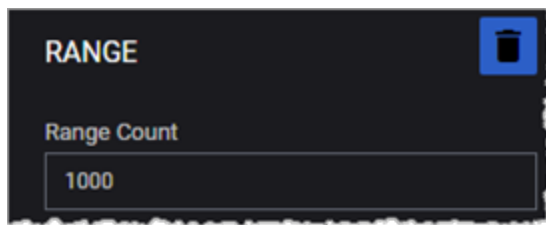
The UE **RANGE** panel provides access to all of the properties that define a UE range.

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

Setting	Description
🗑	Select the **Delete Range** icon to delete this range from your test configuration.
Range Count	Specify the number of UE to configure for this range.
Range settings	Configure detailed UE range settings: • Identification settings on the facing page • UE Security settings on the facing page • UE Settings on page 68 • DRBs Config on page 70 • DNNs Configuration settings on page 71
Objectives	Configure objectives for this range of UEs: UE Test Objective settings on page 76.

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.
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.
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.

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 Settings

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

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.
Send an unsolicited Router Advertisement	Enable this option to send unsolicited ICMP Router Advertisement messages.
IP Address Increment	The value by which the UE IP addresses will be incremented. This refers to all IP addresses assigned to the UE connected to multiple DNNs. When a UE is connected to multiple DNNs, it will have multiple IPs (at least one for each DNN connection). You configure the mapping between DNNs and UE IPs using the UE Range Settings DNNs Config panel
Allowed SSC Modes	The Session and Service Continuity (SSC) Mode for the PDU Sessions that UEs in this range will initiate.

Setting	Description
	The 5G System supports multiple session and service continuity (SSC) modes to support the continuity requirements of various applications and services for the UE. The SSC mode associated with a PDU Session does not change during the lifetime of that Session. The following modes are specified in TS 23.501, section 5.6.9: • **SCC Mode 1**: The network preserves the connectivity service provided to the UE. For PDU Sessions of type IPv4, IPv6, or IPv4v6, the IP address is preserved. • **SCC Mode 2**: The network may release the connectivity service delivered to the UE and release the corresponding PDU Session. For PDU Sessions of type IPv4, IPv6, or IPv4v6, the network may release IP addresses that had been allocated to the UE. • **SCC Mode 3**: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated to allow for better service continuity. For PDU Sessions of type IPv4, IPv6, or IPv4v6, the IP address is not preserved in this mode when the PDU Session Anchor changes. The value you select will be used as the route selection descriptor component value field in the UE Route Selection Policy (URSP). Refer to TS 23.501 and TS 24.526 for detailed information.
Paging Delay (ms)	The time that will elapse before Paging is initiated after UE gets into idle state.
Handover	Enable Handover to configure NR measurement event report values that the UEs can use to trigger handover events. Refer to Handover below below for descriptions of the settings.

Handover

When you enable *Handover* from the UE Settings panel, CuSIM opens a new **Handover** panel that contains the settings described in the table that follows. These settings define report intervals and amounts for the NR measurement event reports and values for Event A3 (Neighbor becomes offset better than SpCell). These settings are fields in the RRC Reconfiguration Message EUTRA report configuration.

Setting	Description
Reporting:	
Report Interval	Select the desired report interval from the drop-down list.
Report Amount	Select the desired report amount. The Report Amount value establishes the limit (if any) on the number of reports to send.

Setting	Description
Event A3:	
A3 Offset RSRP	Specify the RSRP (Reference Signal Receive Power) offset value for Event A3. Event A3 is triggered when a neighbor cell becomes better than a special cell (SpCell) by an offset value. It provides a handover triggering mechanism based upon relative measurement results: in this case, it will be triggered based on the RSRP of a neighbor cell becoming stronger than the RSRP of the SpCell.
Hysteresis	Specify the hysteresis value for this event.
Time to Trigger	The time duration that the measured offset value must be attained before the handover will be triggered.

DRBs Config

You use the DRBs Config panel to configure one or more Data Radio Bearers (DRBs) for each UE Range. From the panel, you can select a DRB Config for editing and add addition DRB configurations.

To configure DRBs for a UE range:

1. Select the range from the **UE RANGES** panel.
2. In the **UE RANGE** panel, select **DRBs**. CuSIM opens the DRBs panel, from which you can add, delete, and select DRBs for the selected range of subscribers.

Setting	Description
DRBs:	
+	Select the **Add DRB** button to add a new DRB for the selected UE range.
🗑	Select the **Delete DRB** button to remove this DRB from the selected UE range configuration.
RLC Mode	RLC Mode identifies the NR RLC Mode. - TM: No RLC Header, Buffering at Tx Only, No Segmentation/Reassembly, No feedback - UM: RLC Header, Buffering at both Tx and Rx, Segmentation/Reassembly, No feedback - AM: RLC Header, Buffering at both Tx and Rx, Segmentation/Reassembly, Feedback (ACK/NACK)
PDCP Uplink/Downlink Sequence Number Size	- PDCP Uplink Sequence Number Size - PDCP Downlink Sequence Number Size
SDAP Uplink Header	Select if 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

Setting	Description
	the 5GCore network and data radio bearer (DRB).
SDAP Downlink Header	Select if SDAP header should be included for this DRB for Downlink Data.

DNNs Configuration settings

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

- DNN panel below
- Session AMBR Configuration settings on the next page
- QoS Flow Panel on page 73

DNN panel

The **DNN** panel contains the configuration settings for an individual DNN. The following table describes the DNN settings:

Setting	Description
DNNs:	
+	Select the **Add DNN** button to add a new DNN to your test configuration.
DNN settings:	
🗑	Select the **Delete DNN** button to remove this DNN from your test configuration.
DNN	Enter the DNN value for this DNN definition. For example: `dnn.keysight.com`.
	A DNN (as is the case with an EPS APN) is composed of two parts:
	• 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.
	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.
	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]`.

Setting	Description
	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. The start value is mandatory. Omitting certain parameters results in behaviors as exemplified below: • `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 UEs will use the DNN values from the pool in a round robin manner. **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).
Local Ipv4 Address	The UE IP address – This is the UE IP Address assigned to the first UE in this UE range during PDU Session Establishment procedure. For the consecutive UEs, **IP Address Increment** defined at **UE Settings** used as an increment value for each UE.
AMBR	Each DNN configuration has its own AMBR settings as defined below Session AMBR Configuration settings.
Qos Flows	The 5G QoS model is based on QoS Flows. A 5G QoS Flow is the finest level of granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receives the same forwarding treatment.

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 bps to Tbps.
Session AMBR Downlink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) downlink rate.

Parameter	Description
Session AMBR Downlink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.

QoS Flow Panel

The 5G QoS model is based on QoS Flows. A 5G QoS Flow is the finest level of granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receives the same forwarding treatment.

Accessing the configuration settings:
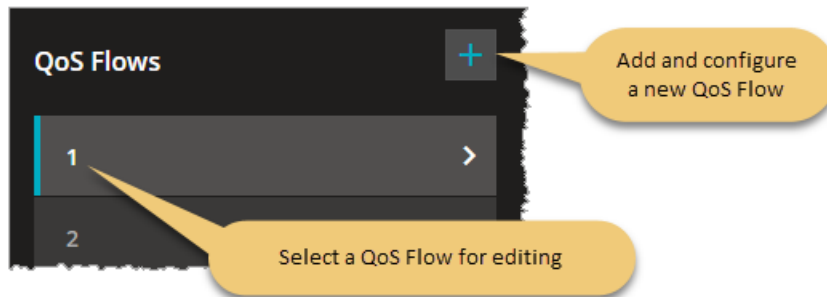
QoS Flow configuration settings

Setting	Description
Is Default	Select 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 will be associated with a QoS Flow.
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.
5QI	Specify the 5QI value (decimal number). 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 oneto-one mapping to a standardized combination of 5G QoS characteristics as specified in TS 23.501, table 5.7.4-1.
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 dedicated network resources related to a QoS Flowlevel Guaranteed Flow Bit Rate (GFBR) value are permanently allocated to the flow.

Setting	Description
Averaging Window	Specify the Averaging window value for this 5GI. Each GBR QoS Flow is associated with an Averaging window. It represents the time duration (specified in milliseconds) over which the GFBR and MFBR are calculated.
QoS Rule Preference	Specify the desired QoS Rule Precedence value for this QFI. The QoS rule precedence value (and the PDR precedence value) determines 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.
DRB	Specify the DRB Id, this QoS Flow should be carried on. Data Radio Bearer with assigned DRB Id, will be created when this QoS Flow is created. Currently one QoS Flow per DRB is supported. Please refer to section DRBs Config
ARP	See QoS Flow ARP configuration settings.
MBR	See QoS Flow MBR configuration settings.
GBR	See QoS Flow GBR configuration settings.

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.

Parameter	Description
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.
Preemption Capability	Select 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.
Preemption Vulnerability	Select 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:

Parameter	Description
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:

Parameter	Description
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.

CHAPTER 11
UE Test Objective settings

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

Each UE UE range defines its own test objectives. The objectives specify the properties of the application traffic that the UEs in the range will generate and transmit over the user plane. Each range can define one or more types of application traffic.

Chapter contents:

User Plane panel

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

Defining user plane objectives

To define application traffic items for your User Plane Objectives:

1. Select the desired UE from the **UE** panel. This opens the Range panel.

2. In the Range panel, click **User Plane** in the Objectives section. This opens the **User Plane** panel.
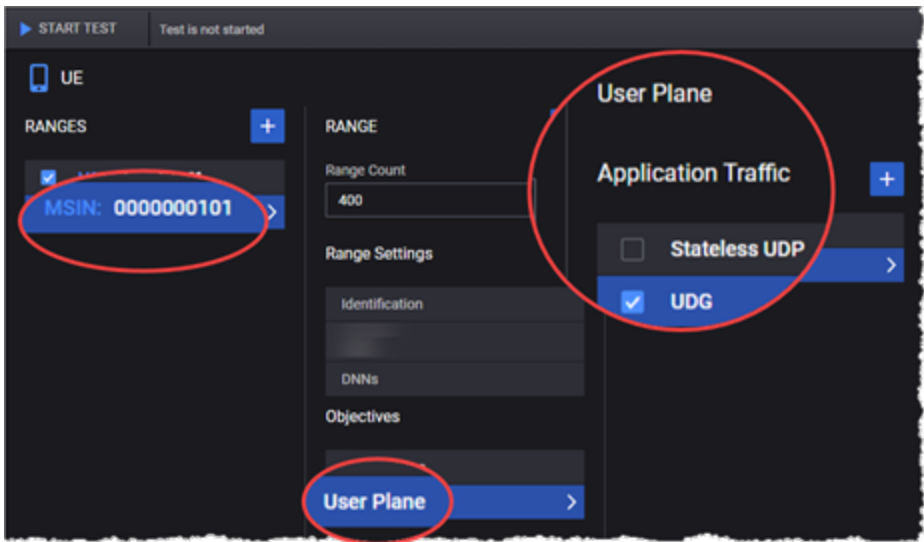
3. Add application traffic items:
   a. In the User Plane panel, click the **Add Objective** icon. This opens the **Data** panel.

   b. In the Data panel, select the desired *Application Type*: Data or USG.

   c. Configure the values, as described in the user plane traffic settings topics.

User Plane traffic settings

Data Traffic

To define the Data application type, select or create an Application Traffic item in the User Plane panel and select Data as the Application Type. This topic describes the Data application traffic parameters.

- Data Traffic settings below
- TCP Settings on the next page
- UDP Settings on the next page
- Application Traffic Flows on page 80

Data Traffic settings

The following table describes the Application Traffic generation parameters for the Data application type.

Parameter	Description
🗑	Click the **Delete Objective** button to remove the application traffic item from your test configuration.
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to **Data**.
Label	Assign this traffic instance a unique label.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
L7 Server IP Address	The IP address of the L7 Server.
L7 Server IP Address Count	The number of L7 Server IP addresses to generate. The L7 Server IP addresses are sequentially increased by 1.
TCP Settings	Select TCP Settings on the next page to configure the TCP settings for this instance of the Data application type.
UDP Settings	Select UDP Settings on the next page to configure the UDP settings for this instance of the Data application type.
Application Traffic Flows	Each Application Traffic entry requires at least one traffic flow definition and can support multiple such definitions. - 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. UI will open the Flow panel where you will select the flow type and configure the flow settings. The Application Traffic Flows are described in Application Traffic Flows on page 80 (below).

TCP Settings

The following table describes the Data Application Traffic TCP settings.

Setting	Description
Min Retransmission Timeout (ms)	The lowest value (in ms) to which the computed RTO timer value can be set. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max Retransmission Timeout (ms)	The highest value (in ms) to which the computed RTO timer value can be set.
Receive Buffer Size	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmission Buffer Size	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	Enable this option to enable the Selective Acknowledgment (SACK) option in the TCP packets.

UDP Settings

The following table describes the UDG Application Traffic UDP settings.

Setting	Description
Receive Buffer Size	The UDP receive buffer size, in bytes.
Transmission Buffer Size	The UDP transmission buffer size, in bytes.
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).

Setting	Description
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).

Application Traffic Flows

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

Parameter	Description
🗑	Click the **Delete Flow** button to remove the flow from your configuration.
Transport Protocol available for Data	Select the transport protocol to carry this application traffic flow. The available protocols are TCP, TLS, and UDP. The transport protocol that you select determines the availability of the Flow Types. <table><tr><th>Protocol</th><th>Supported Types</th></tr><tr><td>TCP</td><td>HTTP Get, HTTP Put, HTTP Post, FTP</td></tr><tr><td>TLS</td><td>HTTP Get, HTTP Put, HTTP Post</td></tr><tr><td>UDP</td><td>UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)</td></tr></table>
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available types are determine by the chosen L4 protocol, and include: • **HTTP GET, HTTP PUT, and HTTP POST** • **UDP Bidirectional** • **FTP**
Port	The server (destination) port used by the flow.
Page Size	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or HTTPS server.
Tx Packets Count	Enter the number of transmit packets to include in the flow. This settings is available for UDP flows only.
Rx Packets Count	Enter the number of Receive packets to include in the flow. This settings is available for UDP flows only.
URL	The URL that is being accessed by the flow's protocol. This setting is available for TCP and TLS protocols only.
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Configuration settings on page 71)

Parameter	Description
QoS Flow ID	The identifier for this quality-of-service flow (QoS Flow).

UDG Traffic

This topic describes the User Data Generator (UDG) Traffic settings.

- Synthetic panel below
- TCP Settings on the facing page
- UDP Settings on the facing page
- Traffic Flow on page 83

Synthetic panel

The following table describes the User Data Generator (UDG) Traffic parameters, which are configured on the **Synthetic** panel.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to **UDG**.
Label	Assign this traffic instance a unique label.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before starting the application traffic flows.
IP Preference	Select the IP address preference: **IPv4** or **IPv6**.
TCP Settings	Refer to TCP Settings on the facing page below.
UDP Settings	Refer to UDP Settings on the facing page below.
Traffic Flow:	
Application Traffic Flows	Each UDG Application Traffic entry requires an NUDG traffic flow entry. NUDG is the UDG peer on the network side. Refer to Traffic Flow on page 83 for descriptions of the NUDG traffic flow settings below.

TCP Settings

The following table describes the UDG Application Traffic TCP settings.

Setting	Description
Min Retransmission Timeout (ms)	The lowest value (in ms) to which the computed RTO timer value can be set. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max Retransmission Timeout (ms)	The highest value (in ms) to which the computed RTO timer value can be set.
Receive Buffer Size	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmission Buffer Size	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	Enable this option to enable the Selective Acknowledgment (SACK) option in the TCP packets.

UDP Settings

The following table describes the UDG Application Traffic UDP settings.

Setting	Description
Receive Buffer Size	The default size of the receive buffer (in bytes). This parameter affects the UDP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmission Buffer Size	The default size of the transmit buffer (in bytes). This parameter affects the UDP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.

Setting	Description
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).

Traffic Flow

The following tables describes the NUDG traffic flow settings.

The following settings are configured on the **Flow** panel, once you select NUDG from the Synthetic panel.

Parameter	Description
Transport Protocol	Select the desired transport protocol to use for this NUDG traffic flow: TCP or UDP..
Out of Band Signaling	Select this option to allow the UDG signaling to be carried on a different path with respect to the data path, directly between the UUDG (UDG client on the UE side) to the NUDG (UDG Network side peer).
	When you enable this option, CuSIM opens an Out of Band Signaling panel in which you specify the address values for the out of band channel.
Port	Enter the port number for this traffic flow.
QoS Flow ID	The identifier for this quality-of-service flow (QoS Flow).

Control Plane panel

You configure Control Plane Objectives for each individual UE range. They are structured as Primary and Secondary objectives, wherein the primary objective defines the event durations and the secondary objective is—in the current release—focused on creating and deleting QoS flows.

Defining control plane objectives

To define the actions for your Control Plane Objectives:

1. Select the desired UE from the **UE** panel. This opens the Range panel.

2. In the Range panel, click **Control Plane** in the Objectives section. This opens the control plane objectives panel.
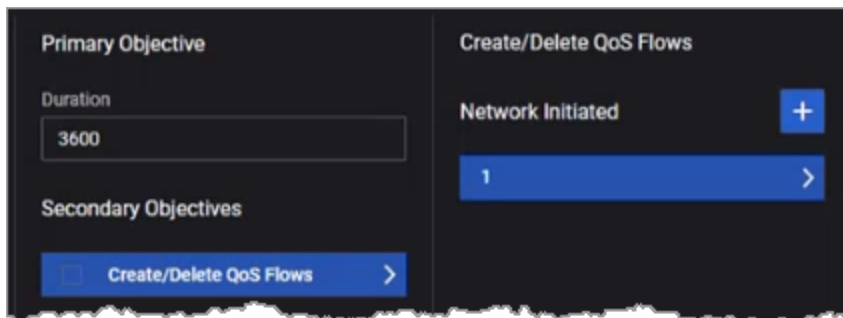
3. Add objectives:

   a. In the control plane objectives panel, specify the desired *Duration* for the **Primary Objective**, in seconds.
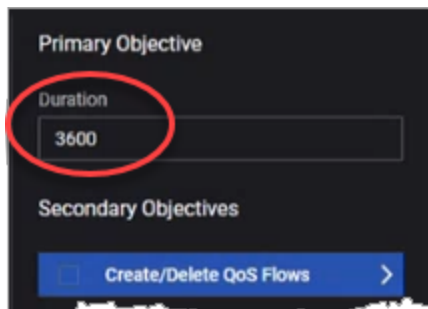
   The *Duration* is the period of time during which the defined secondary objectives are to be sustained.

   b. Click **Create/Delete QoS Flows** to open the configuration panel

   c. Click the **Add Objective** icon to add a Network Initiated objective. This opens the **Objective** panel.

   d. In the **Objective** panel, Configure the values, as described in Create/Delete QoS Flows on the next page.

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.

Secondary Objective parameters

The following table describes the network-initiated QoS flows secondary objective parameters.

Parameter	Description
Create/Delete QoS Flows:	
➕	Select the **Add Objective** button to add an instance of this objective.
Objective:	
🗑	Select the **Delete Objective** button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each UE. If set to zero, it iterates continuously.
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.
Interval	Interval between the triggering of creation and deletion of the QoS flow, in seconds.
DNN	Select the DNN value fror the drop-down list. For example: `dnn.keysight.com`.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

CHAPTER 12
Wireless IP Endpoints

This chapter describes the Wireless IP Endpoints topology, which is an ORAN SIM CE test type that is used when a CuSIM test is configured with a passthrough interface.
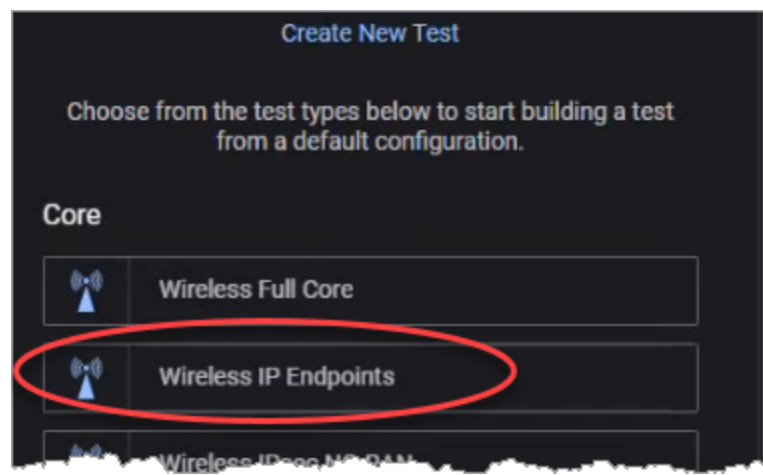
You create the IP endpoints topology by selecting the **Wireless IP Endpoints** test type from the Dashboard page.

Topics:

Wireless IP Endpoints topology

The Wireless IP Endpoints topology is an ORAN SIM CE Core test type that is used by CuSIM when a test is configured with a passthrough interface. This test type is a simple HTTP server that is available to all ORAN SIM CE tests. It can provide an external traffic source for a test and it can also serve as a DUT in a test. The topology comprises an IP Client node and one or more L7 servers. For example:
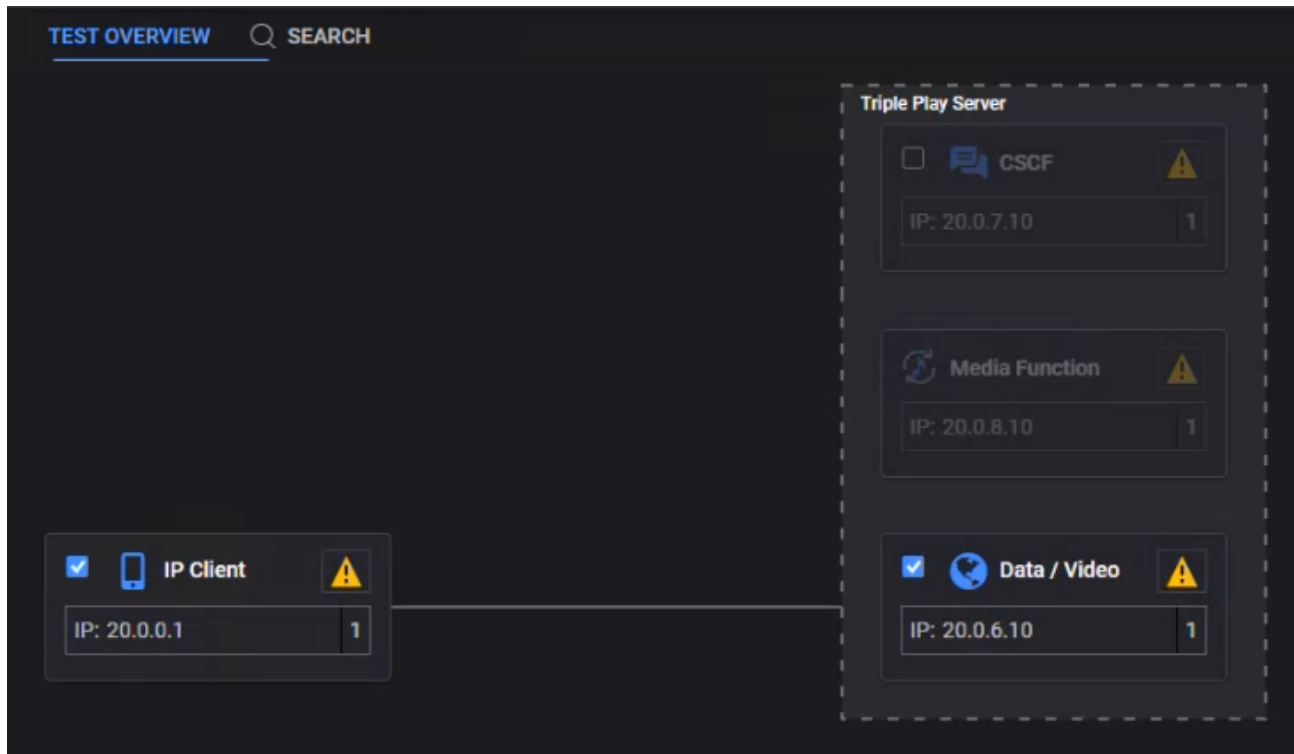
Global Settings

The IP Endpoints Global Settings include parameters that either have overall applicability to the test or can be used (by reference) in the configurations of other nodes in the test topology.

To access the Global Settings:

1. Select the Wireless IP Endpoints **Test Overview** page.

2. Click **Expand** if the Test Overview section is collapsed.

3. Click the Global Settings' **Edit** button:
    ✎

CuSIM opens the **Global Settings** panel from which you can access and configure the following setting:

DNS Settings

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

Setting	Description
DNS Settings:	
Cache Timeout (ms)	The amount of time (in miliseconds) the local DNS stores the address information.
DNS Name Servers:	
＋	Select the **Add DNS Name Server** button to add a new DNS server to your test configuration. Set the IP address of the DNS server.
🗑	Select the **Delete** button to remove the DNS server from your test configuration.

Advanced Settings

The Wireless IP Endpoints Advanced Settings are described in the following tables:

Setting	Description
Overwrite Capture Size for IxStack	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size for IxStack	Set the custom value of the capture size for IxStack.
Enable Capture Circular Buffer for IxStack	Select this option to enable circular buffer capture for IxStack.
Enable Capture On Loopback Interface	Select this option to enable packet capture on the loopback interface.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: • **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

Setting	Description
	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 *Automated Polling Interval* option is disabled. It allows you to create a custom polling interval.
Log Level	Select one of the options: • **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 to debug the application.
Log Tags	Select one or more tags from the drop-down list. 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.
Ignore Offline Agents At Runtime	When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.
IP Client Capture Replay Mode	The CaptureReplayMode that will be used on all ranges of the IP client.

Traffic Settings

The following table describes the settings on the Traffic Settings pane.

Setting	Description
Reserved cores for RTP Tx:	
Enable RTP	Select this option to enable RTP.
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).
Cores	The number of cores reserved for RTP transmission.

Setting	Description
Traffic Control:	
Traffic Control Port	Set the traffic control port. Value should be in range: 1024-65535. By default, it is set to 44556.

UDP Buffer Settings

The following table describes the UDP buffer settings.

Setting	Description
UDP Rx Buffer (bytes)	The size in bytes of the receive buffers for UDP sockets. The values should be in range: 212992-134217728.
UDP Tx Buffer (bytes)	The size in bytes of the transmit buffers for UDP sockets. The values should be in range: 212992-134217728.

Impairment

The following table describes the settings required to define the impairment profile.

Setting	Description
Impairment Profiles:	
+	Select the **Add impairment profile** button to add a new profile to your test configuration.
Impairment Profile:	
🗑	Select 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 default value or overwrite it with your own value.
Action Type	Select an option from the drop-down list. The available option is: **Custom script**.
Script file	This parameter is available only when **Action Type** is set to **Custom script**. It allows you to add a custom script, using the **Upload** button. To remove the script, select the **Clear** button.

Milenage

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

Setting	Description
Milenage Constants	
Override Milenage Constants	Enable this option to override the milenage constants. The following fields are available only when this option is enabled.
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). 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**.

IP Client configuration settings

When you select the IP Client object from the Wireless IP Endpoints topology window, ORAN SIM CE opens the top-level (leftmost) IP Client properties window.
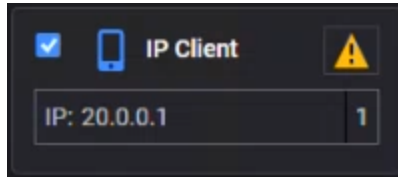
The IP Client configuration settings are described in the following topics:

IP Client Ranges panel

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

- Set the **Distribution Mode**:
  - **All Ranges on All Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UPF node.

    For example, for a test with 2 agents and 3 ranges: range1 on agent1 and agent2, range2 on agent1 and agent2, range 3 on agent1 and agent2.
  - **Round Robin Ranges on Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UPF node.

    For example, for a test with 2 agents and 3 ranges: range1 on agent1, range2 on agent2, range3 on agent1.
- Add a new IP Client range to your test configuration.
- Open a IP Client range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...

IP Client Range panel

You add and select IP Client ranges from the IP Client Ranges panel. When you select an IP address from the **IP Client Ranges** panel, CuSIM opens the **Range** panel, from which you can:

- Select the **Delete Range** button to delete the IP Client range from the test configuration.
- Select the **Create Range Copies** button to create range copies that will be added to your test configuration.
- Designate the range as a **Device Under Test**.

- Use the **Range Settings** panel to configure the node and connectivity settings and the traffic generators for the IP Client range.

IP Client range controls and settings

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

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

Setting	Description
Range:	
🗑	Select the **Delete Range** button to delete this range from your test configuration.
🗐	Select the **Create Range Copies** button to create copies of your range. Also, you can specify the number of ranges to be created.
Device Under Test	Enable this option if your IP Client is a DUT in this test configuration. When this option is not enabled, the IP Client will simulate the IP Client functionality (if it is selected in the Topology window).
Range Count	The number of IP clients in the IP Client range.
Remote Server	The IP address of the remote server.
Range Settings:	
Interface Settings	Each IP Client range requires the configuration of the interface settings, through which an IP Client instance enables connectivity and interaction with other functions in the network. These settings are described in IP Client interface settings.
Timeline	These settings are described IP Client Timeline.
User Plane	These settings are described in IP Client User Plane.

IP Client interface settings

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

Connectivity Settings	Description
IP	*Select the IP address to open the IP configuration panel for editing.*
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.

Connectivity Settings	Description
IP Address Increment	The value by which the IP addresses will be incremented.
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	*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.
Outer VLAN	*Select the check-box to make this option available, then select the Outer VLAN to open the configuration panel for editing.*
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	*This option is visible only when the Outer VLAN check-box is selected.* *Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.*
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.

IP Client Timeline

The following table describes the **Timeline** settings that you configure for each IP Client range.

Setting	Description
Timeline	
Total Test Time (s)	The duration of time (in seconds) for session to be active.

IP Client User Plane

CuSIM provides multiple traffic applications that can be added by selecting the **Add Objective** button.

Parameter	Description
+	Select this button to add a new application traffic objective. The objective can be: • **Stateless UDP** • **Data** • **Voice** • **Video OTT** • **DNS Client** • **ICMP Client** • **Capture Replay** • **Synthetic** • **UDG**
🗑	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 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 Video OTT Traffic.
DNS Client	For the settings required to configure the DNS Clientobjective, refer to DNS Client Traffic.
ICMP Client	For the settings required to configure the ICMP Client objective, refer to ICMP Client Traffic.

Parameter	Description
Capture Relay	For the settings required to configure the Capture Replay objective, refer to Capture Replay.
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to Synthetic Traffic.
UDG	For the settings required to configure the UDG traffic objective, refer to UDG Traffic.

Stateless UDP Traffic

Use the **Stateless UDP** generator if you want to generate IP packets that encapsulate UDP payload. The Stateless UDP generator configuration settings 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 default value or overwrite it with your own value.
Flow Type	This field is set to **uplink** and can not be modified.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Payload Size	The size of the packet payload, in bytes.
Delay (s)	The time to wait before the application traffic flows start.
Destination UDP Port	The start destination port number to place in the UDP header.
Source UDP Port	The source port number to place in the UDP header.

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**.

Parameter	Description
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to **Concurrent Connections**.
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to **Concurrent Connections**.
Connections Rate per Second	Se the value for connections rate per second. This parameter is available only when Objective type is set to **Connections Rate**.
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per IP Client)	Select this option to enable it.
Connection Multiplier (per IP Client)	Set the connection multiplier value.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.
TCP Settings	*Select the pane to open the TCP settings.*
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

Parameter	Description
	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.
Selective Acknowledgments	Select the toggle button to enable this option.

Application Traffic Flows

Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.

- 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. CuSIM will open the Flow panel where you will select the flow type and configure the flow settings.

Refer to Flow for a description of the configuration settings for these traffic flows.

Also, you can add custom parameters, based on your test configuration requirements.

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: • If Optimize Throughput (per IP Client) option is enabled: **TCP**, **TLS**, **QUIC** or **UDP**. • If Optimize Throughput (per IP Client) 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: • 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

Parameter	Description
	client communicates with a server over a bidirectional datagram socket).
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.
Tx Packets Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
RX Packets 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.
Max Transactions per Connection	Set the value for this parameter.
Enable DNS Query Per Connection	Select the check-box to process only one DNS query per TCP connection.

Custom Parameters

In 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
Objective Type	By default, this parameter is set to **Simulated Users** and cannot be changed.
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.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.

Parameter	Description
Call Type	Select the type of call from the drop-down list.
Dial Plan	For the settings required to configure the dial plan, refer to Dial Plan.
Sip Settings:	
Local Port	Set the local port number. You can accept the default value or overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: • **TCP** - Transmission Control Protocol • **TLS** - Transport Layer Security • **UDP** - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	For more details about these settings, refer to Advanced SIP Settings.
RTP Settings	
Local Port	Set the local port number. You can accept the value provided by CuSIM 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.
Audio settings:	For the configuration of audio settings, refer to Audio Settings.
Video Settings:	For the configuration of video settings, refer to Video Settings.
MSRP Settings:	For the configuration of MSRP settings, refer to MSRP Settings.
Advanced Media Settings:	
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: • **None** • **EVS/AMR IPv4** • **NB Codecs IPv6**

Parameter	Description
	• **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
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
MCC	Set the Mobile Country Code (MCC) value.
MNC	Set the Mobile Network Code (MNC) value.
MSIN	Set the MSIN value. The Mobile Subscriber Identification Number (MSIN) is a number that a wireless operator uses to uniquely identify a mobile phone. It is—at most—10-digits long. The MSIN is used (in combination with the MCC and MNC) to form the International Mobile Subscriber Identity (IMSI) number.
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.
Jitter Buffer Settings:	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
Audio Codecs	
➕	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: • **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** The parameters of each audio codec are presented below.

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.

Parameter	Description
Payload Type	Specifies the audio payload type.
Payload Format	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. • **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	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: • **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.
Video Codecs	*This section is available only when **Enable video** is selected*
➕	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 Setttings

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

Parameter	Description
Enable MSRP	Select to enable this option.
MSRP Port	Provide the MSRP port.
MSRP Local domain	Provide the MSRP local domain.

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:

Paramet er	Descrip tion	Value
Accept	IETF RFC 3261	application/sdp,message/cpim
Accept-Contact	IETF RFC 3841	*;mobility="mobile";methods="INVITE"
Accept-Encoding	IETF RFC 3261	gzip

Paramet er	Descrip tion	Value
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
Authentica tion-Info	IETF RFC 3261, IETF RFC 3310	nextnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	<http://wwww.example.com/alice/photo.jpg> ;purpose=icon
Content-Dispositio n	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 23:29:0 0 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg

Parameter	Description	Value
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 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-	IETF RFC	icid-value=1234bc9876e;icid-generated-at=192.0.6.8;orig-

Paramet er	Descrip tion	Value
Charging-Vector	7315	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
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%3Bto-tag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC	Bob <sip:bob@biloxi.com>

Paramet er	Descrip tion	Value
	3261	
Request- Dispositio n	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>
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
Subscripti on-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestam p	IETF RFC 3261	Timestamp
Unsupport	IETF RFC	100Rel

| Paramet er	Descrip tion	Value
ed	3261	
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: • **Digest MD5** • **AKAv1** • **AKAv2** • **ProxyDefined**
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 provided value 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 provided value or enter 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 provided value or enter 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
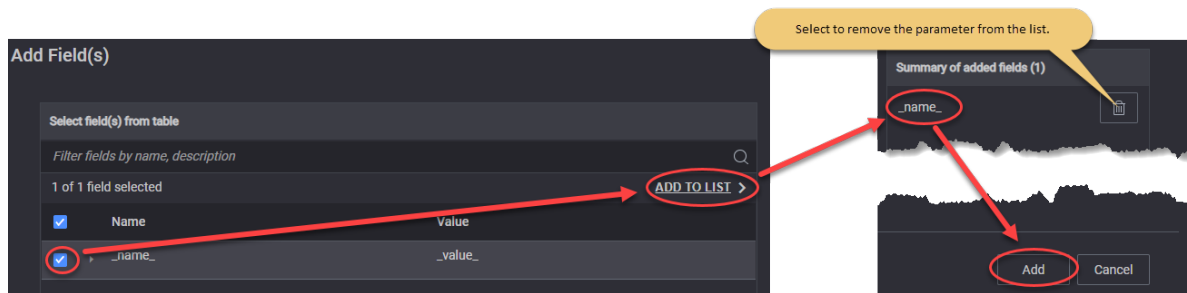
You can add custom parameters as follows:

1. The Custom Parameters panel, select the **Add** button.
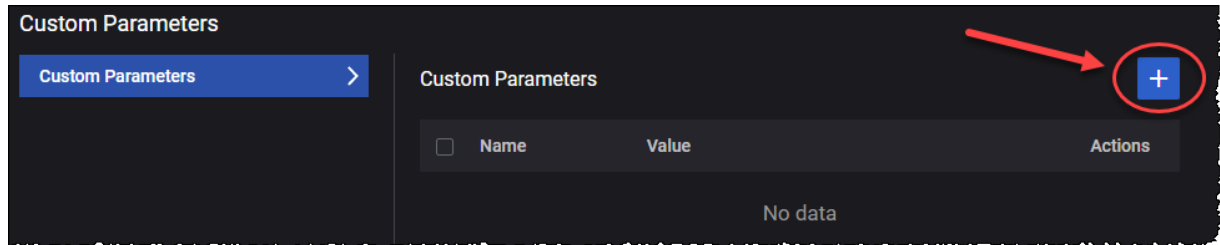
   The Add Field(s) opens.

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 miliseconds before sending SIP INVITE.	1000
DealyBeforeRTP	Delay in miliseconds before RTP session start.	0
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

Parameter	Description	Value
timeoutSIP	Global timeout in miliseconds foe 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 deafult 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: • **hmac-sha-1-96** • **aes-gmac** • **null**
Encryption Algorithm	Select the encryption algorithm: • **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**.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.
Advanced OTT	*Select the* **Open Advanced OTT** *button to enable and configure* *Advanced OTT Settings.*

Advanced OTT Settings

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

Parameter	Description
Application Traffic Flow	Each Application Traffic entry requires at least one Ott traffic flow definition, and can support multiple such definitions. • 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. CuSIM will open the Flow panel where you will select the flow type and configure the flow settings.
Flow:	
🗑	Select this button to remove this flow from your test configuration.
Type	Select the Ott traffic type from the drop-down list. Available options: • **DASH** • **HLS**

Parameter	Description
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 option is enabled, the Play Duration field is disabled and the original playtime is used.
Transport	Select the transport protocol from the drop-down list. Available options: • **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.
Quality Control	These settings are presented in the Quality Control pane.
Advanced Client settings	These settings are presented in the Advanced Client Settings pane.

Quality Control

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

Parameter	Description
Jitter Buffer:	
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.
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: • **Adaptive Bit Rate** • **Quality Predefined Levels** • **Lowest Quality** • **Highest Quality**

Parameter	Description
Number of segments	This field is available and editable only when the Quality Control Mode is set to **Adaptive Bit Rate**.
*Play Profiles: The following settings are available and editable only when the Quality Control Mode is set to **Quality Predefined Levels***.	
[+]	Select this button to add a predefined play profile to your test configuration.
Quality Shift	
[trash icon]	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 • **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
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 <u>Custom Parameters and Custom Headers</u>.
Custom Headers	For more details, refer to <u>Custom Parameters and Custom Headers</u>.

Custom Parameters and Custom Headers

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.
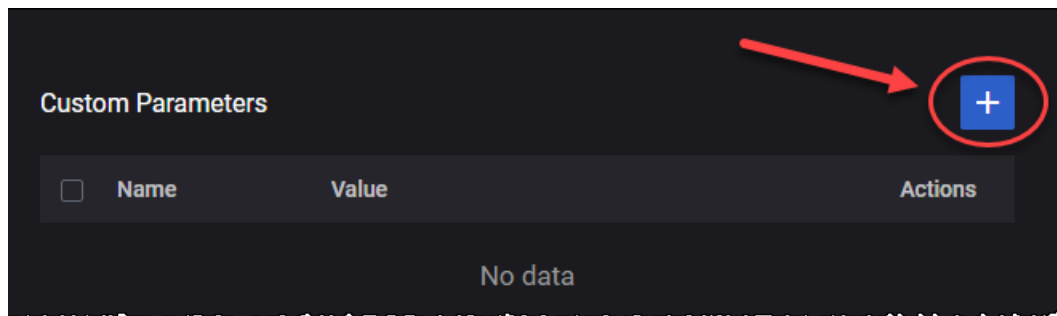
   The Add Field(s) opens.

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.

DNS Client Traffic

The following table describes the DNS Client Traffic parameters.

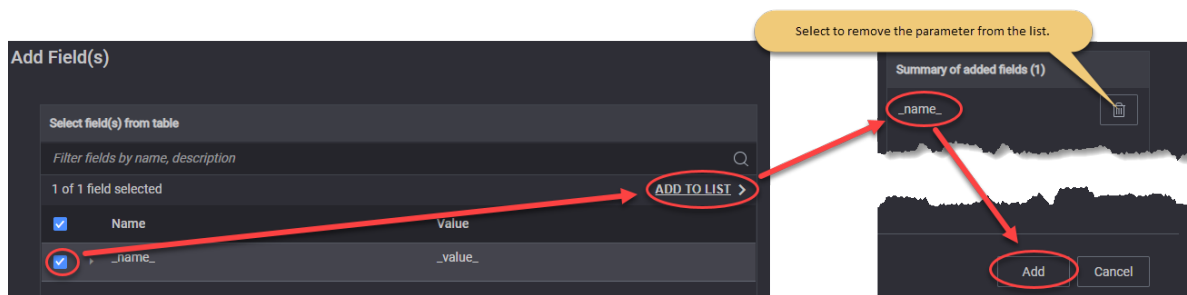| Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to **DNS Client**.
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Objective Type	By default, this parameter is set to **Simulated Users** and cannot be changed.
Connection multiplier (per IP Client)	Set the value for the connection multiplier.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.
Application Traffic Flows	Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions. • 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. CuSIM will open the Flow panel where you will select the flow type and configure the flow settings. Refer to Flow for a description of the configuration settings for these traffic flows. Also, you can add custom parameters, based on your test configuration requirements.

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.

Parameter	Description
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: • **A** • **AAAA** • **CNAME** • **TXT** • **PTR** • **NS**
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.

Custom Parameters
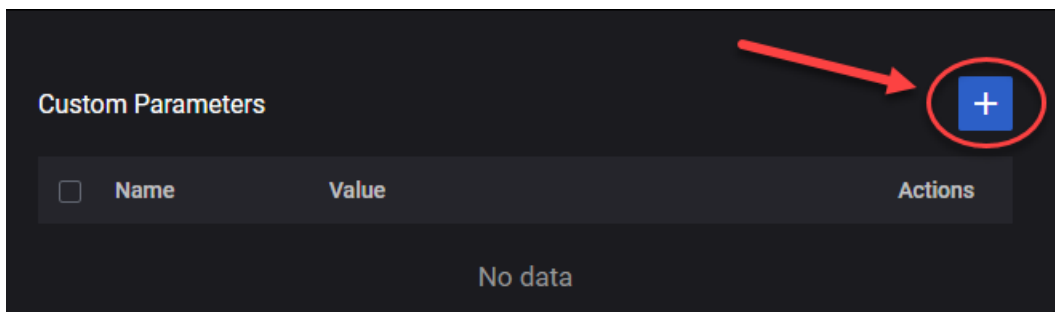
You can add custom parameters as follows:

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

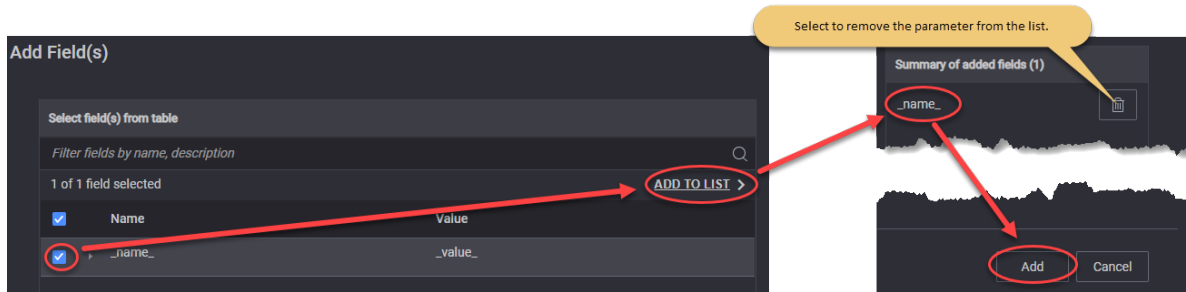   The Custom Parameters panel opens.

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.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.
Objective Type	By default, this parameter is set to **Simulated Users** and cannot be changed.
Traffic Flow	Refer to Traffic Flow (below) 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
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.

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**.
Label	Set the label name. You can accept the default value or overwrite it with your own value.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
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.
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 after all IPs have been configured.

Filter parameters

The following table describes the Filter object parameters.

Parameter	Description
Filter	
+	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).

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.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: **IPv4** or **IPv6**.
TCP Settings	
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

Parameter	Description
	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).
Selective Acknowledgments	If necessary, enable this option.
UDP Settings	
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
Flow	
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.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Client Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
Server Burst Interval (ms)	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
Server Timeout (ms)	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 User Data Generator (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.

Parameter	Description
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: **IPv4** or **IPv6**.
TCP Settings	
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).
Selective Acknowledgments	If necessary, enable this option.
UDP Settings	
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
Flow	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: **TCP** or **UDP**.
Out of Band Signaling	*Select this check-box to enable OOB signaling. More details about the required parameters [here](.)*
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
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.

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.

Parameter	Description
Port	Set the used port.

The following table describes the UDG Traffic Parameters.

Parameter	Description
UGD Test Type	Select the test type from the drop-down list. Available options: **Transmission** or **Ping-pong**. For each test type, the parameters are described below.
Transmission	
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Server Burst Interval (ms)	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
Ping-pong	
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: **Milisecond** 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.

Triple Play Server configuration settings

In a CuSIM test, the Triple Play Server has three important components:

- Call Session Control Function (CSCF) – responsible for controlling sessions between endpoints and applications.
- Media Function
- Data/Video

The configuration settings for these three components are described in the following topics:

CSCF Range panel

When you select the Call Session Control Function (CSCF) IP address from the **CSCF Ranges** panel, CuSIM opens the **Range** panel, from which you can select **CSCF Settings** to configure the node and connectivity settings for the CSCF range. Also, you can designate the range as a **Device Under Test**.

CSCF range controls and settings

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

Setting	Description
Device Under Test	Enable this option if your CSCF is a DUT in this test configuration. When this option is not enabled, the Wireless IP Endpoints topology will simulate the CSCF functionality (if it is selected in the Topology window).
P-CSCF Node Settings	
Domain	Set the domain name.
Port	Set the port number. You can accept the default value or overwrite it with your own value.
Authentication Settings	
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**.
Interface Settings	
IP	*Select the IP address to open the IP configuration panel for editing.*
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.

Setting	Description
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Outer VLAN	*Select the check-box to make this option available, then select the Outer VLAN to open the configuration panel for editing.*
VLAN ID	The VLAN identifier.
Inner VLAN	*This option is visible only when the Outer VLAN check-box is selected.* *Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.*
VLAN ID	The VLAN identifier.

Media Function Range panel

When you select the Media Function's IP address from the **Media Function Ranges** panel, ORAN SIM CE 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
IP:	
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).
MAC:	
MAC 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.
VLAN:	
Outer VLAN	Select the check-box to make this option available, then select the Outer VLAN to open the configuration panel for editing.

Connectivity Settings	Description
Outer VLAN ID	The VLAN identifier.
Inner VLAN	This option is visible only when the Outer VLAN check-box is selected. Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.
Inner VLAN ID	The VLAN identifier.

Data/Video configuration settings

The Data/Video configuration settings are described in the following topics:

Data/Video Ranges panel

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

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

For example ...
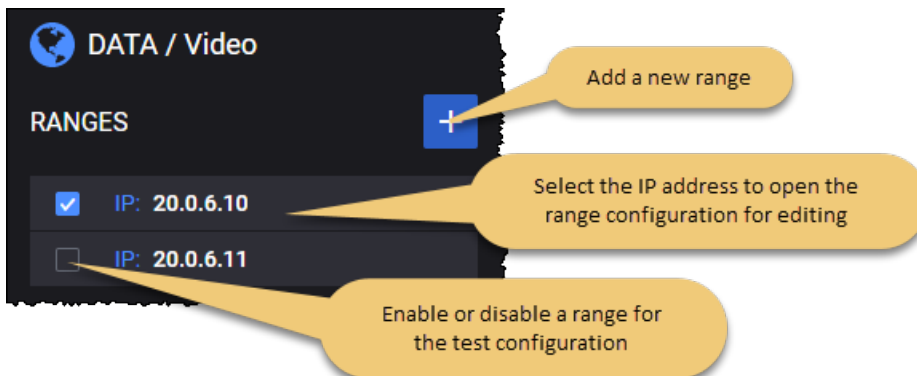
Data/Video Range panel

You add and select Data/Video ranges from the Data/Video Ranges panel. When you select a Data/Video's IP address from the **Data/Video Ranges** panel, the **Range** panel opens, from which you can:

- Select the **Delete Range** button to delete the Data/Video range from the test configuration.
- Select the **Create Range Copies** button to create range copies that will be added to your test configuration.
- Designate the range as a **Device Under Test**.
- Use the **Range Settings** panel to configure the node and connectivity settings and the traffic generators.

Data/Video range controls and settings

Each Data/Video range is identified by a unique IP address. You can add and delete Data/Video ranges as necessary to support your test objectives.

The following table describes the available **Range** configuration options for each Data/Video range.

Setting	Description
Range:	
🗑	Select the **Delete Range** button to delete this range from your test configuration.
🗐	Select the **Create Range Copies** button to create copies of your range. Also, you can specify the number of ranges to be created.
Device Under Test	Enable this option if your Data/Video is a DUT in this test configuration. When this option is not enabled, the Wireless IP Endpoints topology will simulate the Data/Video functionality (if it is selected in the Topology window).
Range Count	Set the value for the range count.
Range Settings:	
Interface Settings	These settings are described in [Data/Video interface settings](#).
User Plane	These settings are described in [Data/Video User Plane](#).

Data/Video interface settings

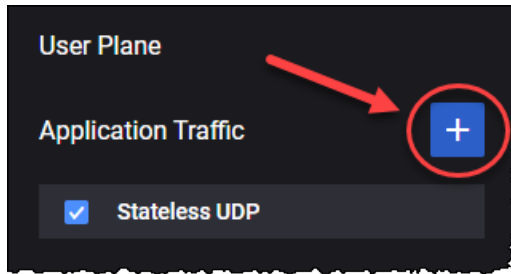The following table describes the **Connectivity Settings** that you configure for each Data/Video range.

Connectivity Settings	Description
IP	*Select the IP address to open the IP configuration panel for editing.*
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

Connectivity Settings	Description
	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	*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.
Outer VLAN	*Select the check-box to make this option available, then select the Outer VLAN to open the configuration panel for editing.*
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	*This option is visible only when the Outer VLAN check-box is selected.* *Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.*
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.

Data/Video User Plane

The Wireless IP Endpoints topology provides multiple traffic application that can be added by selecting the **Add Objective** button.

Parameter	Description

➕	Select this button to add a new application traffic objective. The objective can be:
	  • **Stateless UDP**
	  • **Data**
	  • **Voice**
	  • **Video OTT**
	  • **DNS Server**
	  • **Capture Replay**
	  • Synthetic
	  • UDG

🗑	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 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 Video OTT Traffic.
DNS Server	For the settings required to configure the DNS Server objective, refer to DNS Server Traffic.
Capture Relay	For the settings required to configure the Capture Replay objective, refer to Capture Replay.

Parameter	Description
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to Synthetic Traffic.
UDG	For the settings required to configure the UDG traffic objective, refer to UDG Traffic.

Stateless UDP Traffic

Use the **Stateless UDP** generator if you want to generate IP packets that encapsulate UDP payload. The Stateless UDP generator configuration settings for the downlink 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 default value or overwrite it with your own value.
Flow Type	This field is set to **downlink** and can not be modified since on the Data/Video 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.
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.

Data Traffic

The following table describes the DN 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.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest

Parameter	Description
	TCP segment that the IP device can transmit as a single, unfragmented unit.
TCP Settings	*Select the pane to open the TCP settings.*
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.
Selective Acknowledgments	Select the toggle button to enable this option.

Application Servers

Each Application Traffic entry requires an application server definition, and can support multiple such definitions.

- To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.
- To add another application server, click the **Add Server** button. The Server panel will open from which you will select the server type and configure the server settings.

Refer to Server (below) for a description of the configuration settings required by the application server.

Also, you can add custom parameters, based on your test configuration requirements.

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: • 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.

Custom Parameters

In 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.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.
Call Type	Select the type of call from the drop-down list.
Dial Plan:	*For the settings required to configure the dial plan, refer to Dial Plan.*
Sip Settings:	
Local Port	Set the local port number. You can accept the value provided by CuSIM or overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: • **TCP** - Transmission Control Protocol • **TLS** - Transport Layer Security • **UDP** - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP	For more details about these settings, refer to Advanced SIP Settings.

Chapter 12 Wireless IP Endpoints

Parameter	Description
Settings	
RTP Settings	
Local Port	Set the local port number. You can accept the value provided by CuSIM 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.
Audio settings:	For the configuration of audio settings, refer to <u>Audio Settings</u>.
Video Settings:	For the configuration of video settings, refer to <u>Video Settings</u>.
MSRP Settings:	For the configuration of MSRP settings, refer to <u>MSRP Settings</u>.
Advanced Media Settings:	
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: • **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.
Jitter Buffer Settings:	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
Audio Codecs	
➕	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: • **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** The parameters of each audio codec are presented below.

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.

Parameter	Description
Payload Type	Specifies the audio payload type.
Payload Format	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. • **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	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: • **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.
Video Codecs	*This section is available only when **Enable video** is selected*
➕	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 Setttings

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

Parameter	Description
Enable MSRP	Select to enable this option.
MSRP Port	Provide the MSRP port.
MSRP Local domain	Provide the MSRP local domain.

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 headers 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

Parameter	Description	Value
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	IET RFC 3261, IETF RFC 3310	nextnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	<http://wwww.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>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC 3261	3600
Feature-Caps	IETF RFC 6809,	+3gpp.trf=sip:trf3.operator3.com

Parameter	Description	Value
	3GPP TS 24.229	
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 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-	IETF RFC	userC@example.com

Parameter	Description	Value
Missing	5360	
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
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%3Bto-tag%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

Parameter	Description	Value
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
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: • **Digest MD5** • **AKAv1** • **AKAv2** • **ProxyDefined**
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.
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 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.
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.

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 default value or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.

Parameter	Description
OTT Servers:	
![+]	Select this button to add an OTT server to your test configuration.
![trash]	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 default value or overwrite it with your own value.
Transport	Select the transport protocol. The available options are: • **HTTP** • **HTTPS** • **HTTP/QUIC**
Port	Set the port number. You can accept the default value or overwrite it with your own value.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
Streams	*Refer to [Streams](#) (below) 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.

Streams   ![→]

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

Parameter	Description
![+]	Select this button to add a stream to your test configuration.
![trash]	Select this button to remove the stream from the test configuration.
Stream Name	Set the stream name. Each server is identified by a unique name. You can accept the default value or overwrite it with your own value.
URL	Set the URL path.
Type	Select the stream type from the drop-down list:

Parameter	Description
	• **Real** • **Synthetic**
Protocol	Select the protocol from the drop-down list: • **Apple 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:	*Set the quality value for each level.*
➕	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

In 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.
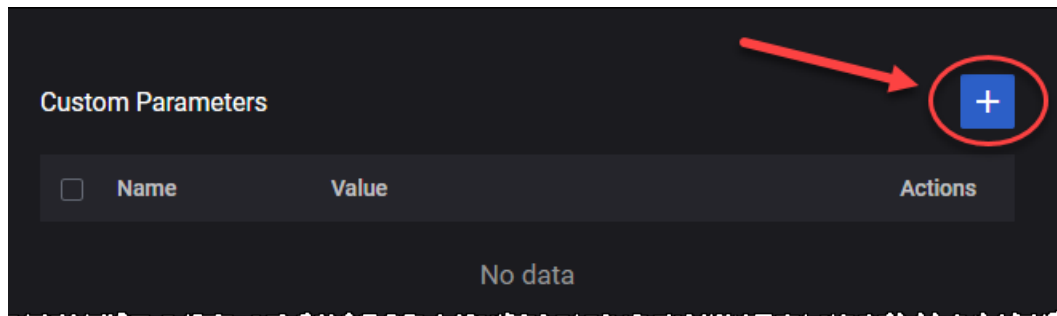
The Add Field(s) opens.

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.

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 default value or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.
DNS Servers:	
+	Select this button to add an DNS server to your test configuration.

Parameter	Description
🗑	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 default value or overwrite it with your own value.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
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.

Zone Manager ⏏

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 default value or overwrite it with your own value.
Master Server	Provide the value for the master server.
Resource Records (RRs)	
➕	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: • **A** • **AAAA**

Parameter	Description
	• **CNAME** • **TXT** • **PTR** • **NS**
Hostname	Set the hostname.
Address	Provide the address.

Custom Parameters

You can add custom parameters as follows:

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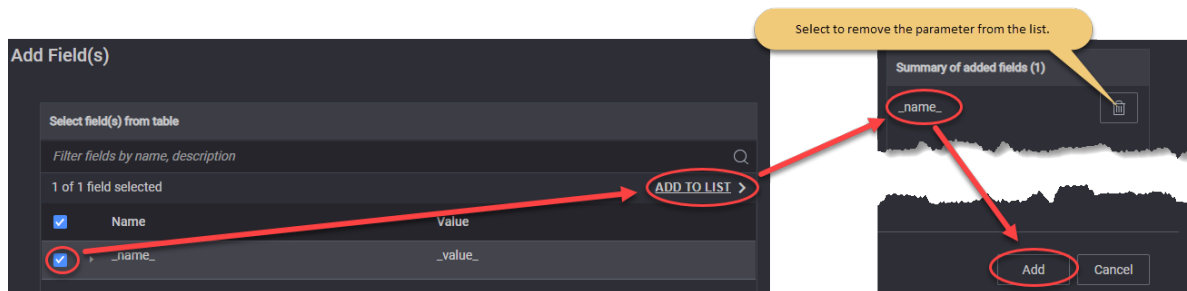

The Custom Parameters panel opens.

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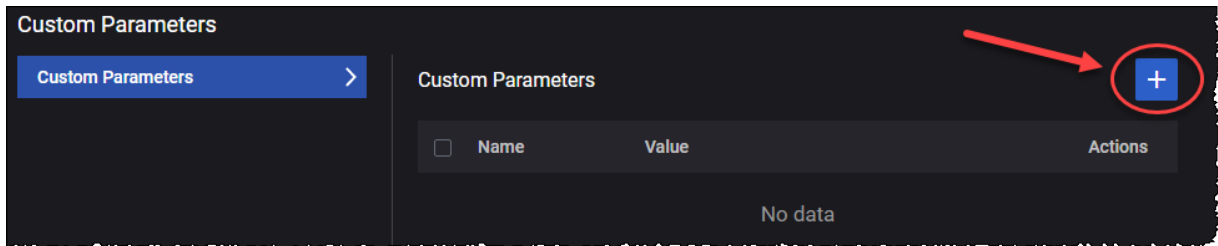
The Add Field(s) opens.

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 …

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**

Parameter	Description
	Replay.
Label	Set the label name. You can accept the default value 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.
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	Attempt to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is **true** (option enabled).

The following table describes the Filter object parameters.

Parameter	Description
Filter	
+	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**

Parameter	Description
	(option disabled).
Override IP Address	*Select the toggle button to enable it. When enabled, Source IP Address and Source IP Address Count fields become available.*
Source IP Address	The source IP address to place in the IP packet.
Source IP Address Count	The source 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.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
TCP Settings	
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

Parameter	Description
	Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	If necessary, enable this option.
UDP Settings	
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
Flow	
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.

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**.

Parameter	Description
Label	Set the label name. You can accept the default value or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.
TCP Settings	
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).
Selective Acknowledgments	If necessary, enable this option.
UDP Settings	
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

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).

The following table describes the Traffic Flow parameters.

Parameter	Description
Flow	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: **TCP** or **UDP**.
Out of Band Signaling	*Select this check-box to enable OOB signaling. More details about the required parameters here.*
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.
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.

CHAPTER 13
Manage and use test sessions

When you create a new test, CuSIM 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

Once a test is configured (for details, refer to <u>Create a new test config on page 17</u>), 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.
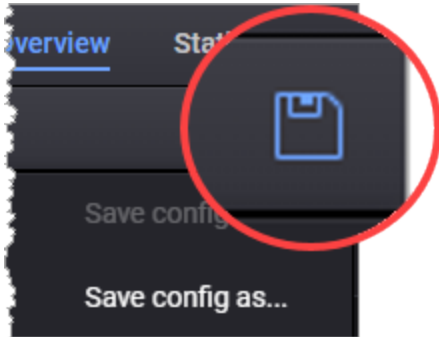
2. Choose one of the following:
    a. Either **Save config** to quickly save your test configuration.
    b. Or, **Save config as** to save your test configuration with a specific name; then enter a name for the test configuration and click the **Save as** button.
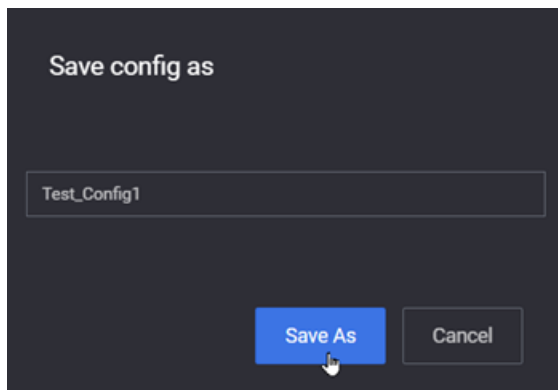
Manage test sessions

Managing saved tests is done on the **Browse Configs** page. To access the page, click the **Browse Configs** button from the main CuSIM Dashboard.
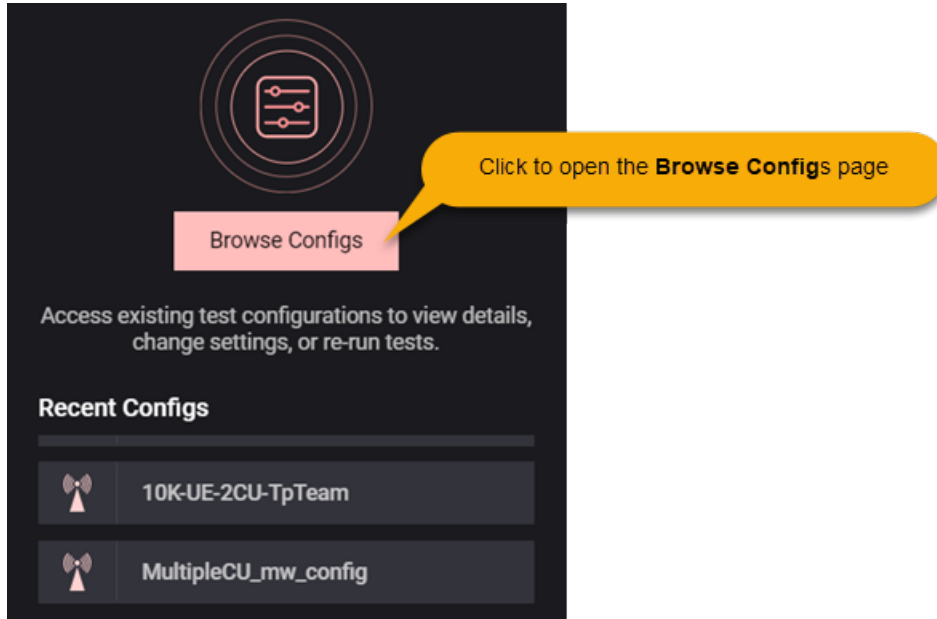
The **Recent Configs** list contains default configurations plus previously loaded configurations. If you select one of the configurations (by clicking it) a new session is created with this configuration loaded inside of it.

> **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,CuSIM displays your test configurations suite, offering you details on the specific test configuration and allowing you to delete it or to export it.

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

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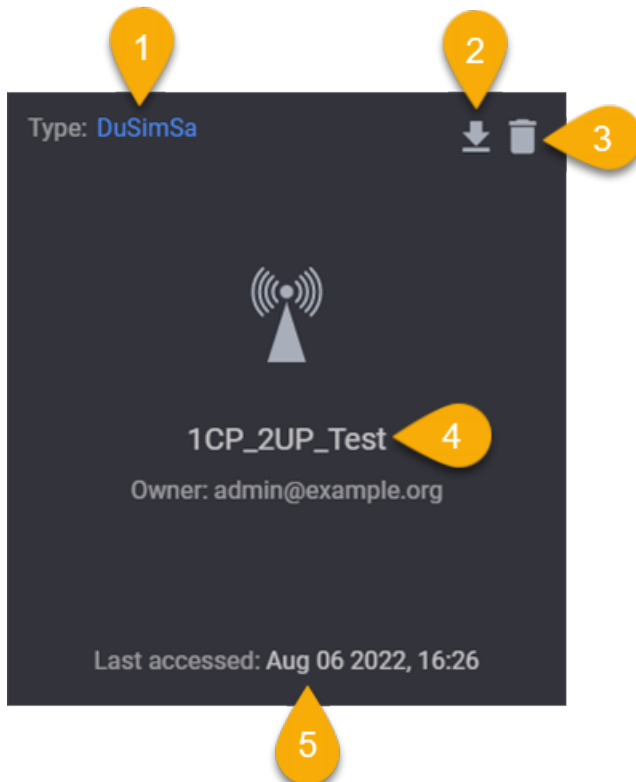
1	Indicates the test type
2	Click the button to export the test configuration
3	Click the button to delete the test configuration
4	Details on the test name and test owner
5	Timestamp of the last test session

Test configurations displayed as rows

	1	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 *system*.
	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.
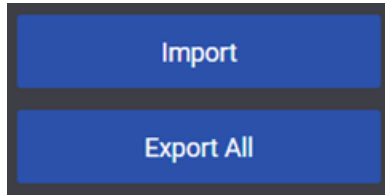
Import test configurations

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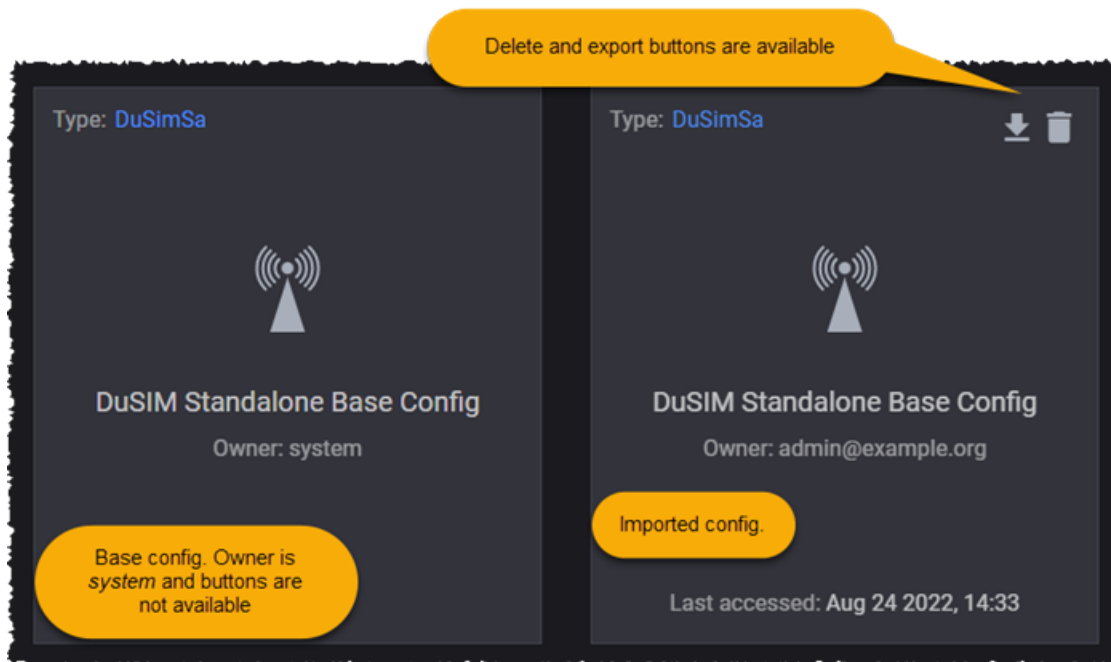
If a test is imported twice with the same name, the second time the test name will be displayed with details about the date and time of the import.

Details about the date and time are added to the name of the test when it is imported the second time.

The name of the test when it was imported the first time.

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 CuSIM 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 CuSIM 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.
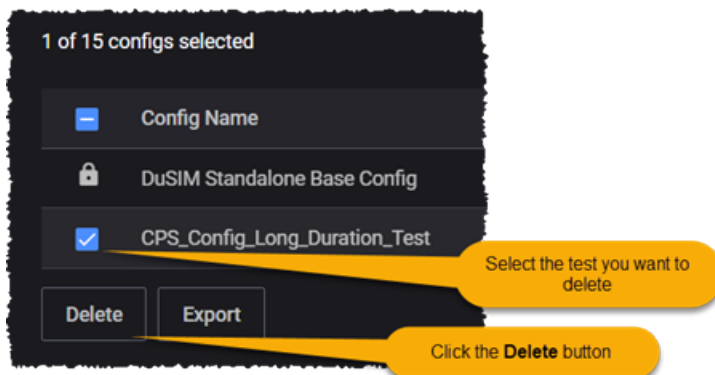
When in tile view mode, click the **Delete** button from the test tile .
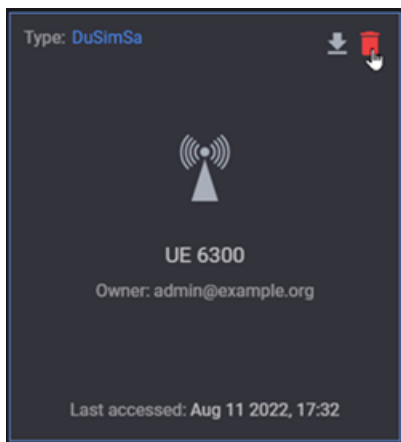
This will delete the configuration from the database, but not the session itself.

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 .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 .0 opens a confirmation dialog.
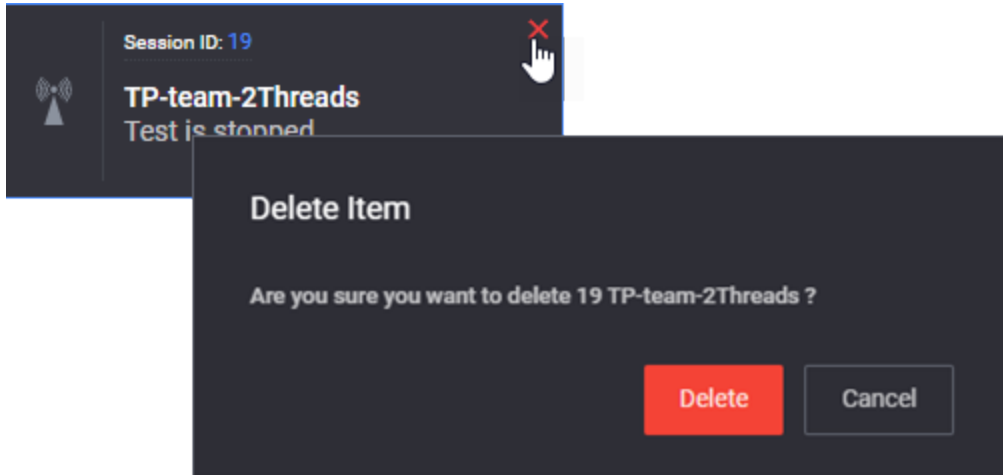
3. Select **Delete** to confirm the action.

CHAPTER 14
Manage CuSIM licenses

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

Chapter contents:

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 CuSIM web UI.

License Manager

The first time you use CuSIM, you need to active at least one license. You activate and manage your licenses using the CuSIM **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 CuSIM License Manager:

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

Activate a license

To activate one or more CuSIM licenses:

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

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

Deactivate a license

To activate one or more CuSIM 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 CuSIM licenses:

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

Reserve a license

To reserve one or more CuSIM licenses:

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

2. Select the **Manage Reservation** icon.
   CuSIM 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 CuSIM 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 CuSIM license operations:

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

2. Select **Offline operations**.
   CuSIM 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 CuSIM 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 CuSIM web UI:

1. Log in the CuSIM 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 CuSIM web UI:

1. Log in the CuSIM 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 CuSIM licenses:

1. From the Setting menu (⚙), select **Application Settings**.
   CuSIM 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 15
Manage CuSIM users

Managing the users who can access the application is one of the primary CuSIM 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 179](#)

User categories

CuSIM 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 CuSIM application must have a user account. To add a user:

1. Select the settings menu (⚙) and then select **User Management**.
   CuSIM 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.
   CuSIM 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.
       CuSIM 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**.
    CuSIM 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.
    CuSIM 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**.
    CuSIM 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**.
    CuSIM 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**.
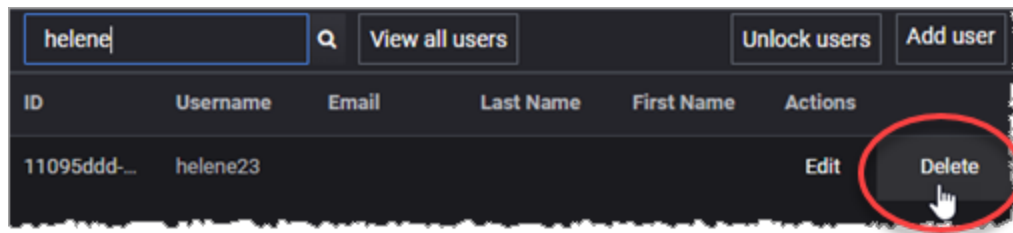
5. CuSIM opens a confirmation dialog.

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 it function and usage. For more information about the **Access Control** options and configuration, refer to the official [Keycloak documentation](#).

CHAPTER 16
CuSIM 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 182](#)
- [Events notifications on page 182](#)
- [Technical Support and Application Help on page 182](#)

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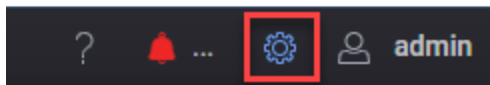
The gear icon opens the Settings menu, which provides access to a number of application and system settings, administrative functions, and application resources:

Setting	Description
License Manager	Select this option to open the [License Manager on page 174](#) window.
Agent Management	Select this option to open the [Agent management on page 39](#) window.
Resource Library	The location to which you can import, and from which you can access, your various application resources, including: packet captures, CA certificates, and objects (SIP, HTTP, Media, Flow, and other).
Software Updates	Select this option to open the **Software Updates** window. To update to a newer version, do the following: 1. Open the **Settings** menu (⚙) and click on **Software Updates**. 2. Click **Select Packages For Upload** and open the folder containing the upgrade file. 3. Select the upgrade file and click **Open**. 4. Click **Start Update** to initiate the update process. 5. If needed, you can remove the update packages from the update section by clicking **Reset Current Changes**.

Setting	Description
Application Settings	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**: • **External License Server** - select this option to set an external license server. • **Embedded License Server** - the license server that is included in CuSIM MW. Refer to License Manager on page 174 for information about activating and managing licenses.
Logs Level	You use the Logs Level setting to view and change the log level that it set for the CuSIM Controller. The logs level determines the type of data that are written to the log files: • Error: Designates messages indicating that an error has occurred that impacts application stability. • Warn: Designates messages indicating that an error has occurred that potentially impacts application stability. • Info: Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug: Designates fine-grained informational events that are most useful for debugging the application.
Data Migration	Allows you to export selected data (such as authentication data and configs) and to import controller data from a migrate package.
System Monitor	The ORAN SIM CE System Monitor provides tools for monitoring and managing the application's system health. There are two such tools: • Controller Health: Displays CPU, Memory, and storage utilization data over selectable periods of time. • System Cleanup: Displays the size of the Logs, Diagnostics, and Migration data storage files and permits deletion of any of these.
User Management	Application Administrators use the User Management settings for all aspects of user management. For detailed information, refer to Manage CuSIM users on page 177.

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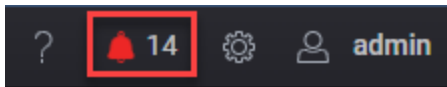
The events icon shows the number of event notifications that have been received, and the color of the icon reflects the nature of the events. For example, if the events list contains any Error events, the icon will be red.

Refer to 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 for more information about collecting diagnostics data.

CHAPTER 17

Troubleshooting

CuSIM 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 CuSIM provides are notification and event management, messages displayed during test execution, test diagnostics data, and log files.

Chapter contents:

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 CuSIM instance. The icon and the counter are visible from all the pages of the CuSIM 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 *error* notification indicates that an error has occurred that impacts application stability. The application is possibly in an unstable or indeterminate state, and the should either be restarted or should carry out error recovery or re-initialization routines.
WARNING		A *warning* notification indicates an error has occurred that potentially impacts application stability.
INFO		An *info* notification indicates a general-purpose notification, such as logging data or a heartbeat indicator.

To view more details on the triggered events, select the notifications icon. The **Events** window is displayed.
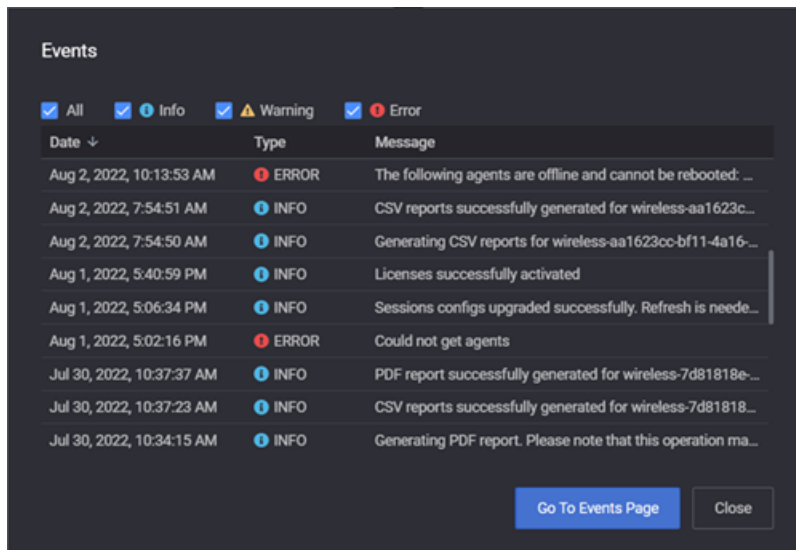
Here you can view details on the registered events regarding the logging date, their severity type and description. You can choose to display all events or certain types of events, based on their severity, by selecting or clearing the associated check-box.

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

Collect Diagnostics

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

To collect diagnostics, do the following:

1. Click on **Collect Diagnostics** in the **Settings** menu. Select the Help icon in the title bar. The **Diagnostics** window appears.
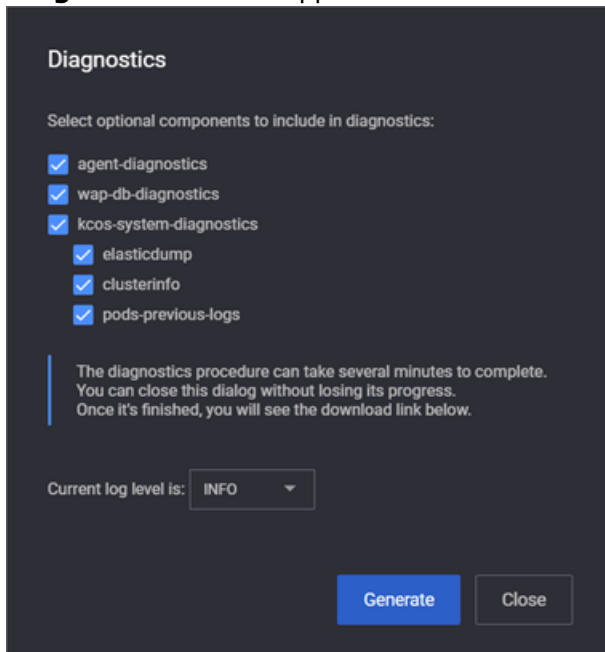
2. If needed, select the optional components to include in the diagnostics report.

3. Select the log level used to collect diagnostics. Available options are:

   - **ERROR**- Designates messages indicating that an error has occurred that impacts application stability.

   - **WARN** - Designates messages indicating that an error has occurred that potentially impacts application stability.

   - **INFO** - Designates informational messages that highlight the progress of the application at coarse-grained level.

   - **DEBUG** - Designates fine-grained informational events that are most useful for debugging the application.

4. Click **Generate**. The diagnostics procedure can take several minutes to complete. Once it is finished, a download link will be displayed.

5. Select the download link to retrieve the diagnostics report.

Index

KEYSIGHT