

Keysight Open RAN Simulators, Cloud Edition 2.0

CoreSIM

User Guide

Notices

Copyright Notice

© Keysight Technologies 2022–2023

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

Warranty

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

Technology Licenses

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

U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at <http://www.keysight.com/find/sweula>. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose

commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data. 52.227-14 (June 1987) or DFAR 252.227-7015 (b)(2) (November 1995), as applicable in any technical data.

Contacting Us

Keysight headquarters

1400 Fountaingrove Parkway

Santa Rosa, CA 95403-1738

www.ixiacom.com/contact/info

Support

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

Table of Contents

Chapter 1 Introduction	10
Objectives-based testing	10
UI overview	10
Additional information and resources	12
Chapter 2 Initial administrator login	14
Chapter 3 User login and logout	18
Chapter 4 Build and run a test	20
Create a new test config	20
Configure the test	21
Start the test	22
View real-time test results	23
Test results	23
Chapter 5 Assign and manage agents	24
About traffic agents	24
Assigning agents to nodes	24
Agent management	25
Network Management	28
Chapter 6 CoreSim tests: configuration settings	30
Global Settings	33
Global Settings panel	36
Node Start/Stop Rates	36
DNS Settings	37
Advanced Settings	37
DNNs panel	40
DNN configuration settings	40
Session AMBR configuration settings	44

ePCO configuration settings	44
Traffic Control Settings configuration	46
Impairment	47
QoS Flows panel	48
QoS Flow configuration settings	48
QoS Flow Packet Filter configuration settings	51
QoS Flow Max Packet Loss Rate settings	53
QoS Flow ARP configuration settings	53
QoS Flow MBR configuration settings	54
QoS Flow GBR configuration settings	54
Milenage	54
Customer Parameters	55
CA Certificates	55
UE configuration settings	56
UE Ranges panel	56
UE Range panel	57
Range Settings	58
UE Identification settings	59
UE Security settings	60
UE Settings settings	63
UE Subscribed AMBR settings	70
DNNs Config	70
SMS Configuration	73
Untrusted WiFi Settings	73
Network Slicing settings	75
UE NSSAI settings	76
UDM SNSSAI Mappings	77
Objectives	77
Control Plane Objective	78
About primary objectives	78
Primary Control Plane Objective	80

Secondary Control Plane Objective	82
Handover	83
Paging	85
Enter/Exit Idle	86
Create/Delete QoS Flows	87
Create/Delete PDU Sessions	89
SMS	90
User Plane Objectives	91
Stateless UDP Traffic	92
Data Traffic	94
Voice Traffic	98
Video OTT Traffic	113
DNS Client Traffic	116
ICMP Client	119
Capture Replay	120
Synthetic	122
UDG	124
Predefined Applications Traffic	128
Applications	130
Application Advanced Settings	133
TCP Settings	135
TLS Settings	136
RTP Settings	138
DN configuration settings	138
DN Ranges panel	139
DN Range panel	139
DN N6 interface settings	140
DN routes settings	141
DN User Plane	142
DN Stateless UDP Traffic	143
DN Data Traffic	144

DN Voice Traffic	147
DN Video OTT Traffic	158
DN DNS Server Traffic	161
DN Predefined Applications Traffic	163
DN Capture Replay	164
DN Synthetic	166
DN UDG	168
IMS configuration settings	170
CSCF Range panel	170
Media Function Range panel	171
RAN/Untrusted AP configuration settings	171
gNodeB	172
gNodeB Ranges panel	173
gNodeB Range settings	176
gNodeB node settings	177
gNodeB NSSAI settings	180
gNodeB N2 interface settings	181
gNodeB N3 interface settings	185
eNodeB	189
eNodeB Ranges panel	189
eNodeB Range Settings	193
eNodeB Node Settings	194
S1-U Interface Settings	195
S1-MME Interface Settings	196
UNAP	198
UNAP Ranges panel	198
UNAP Range Settings	199
Passthrough interface settings	200
SEG/N3IWF & CoreSim configuration settings	202
Core settings	203
N6/SGi interface settings	203

AMF Ranges configuration settings	205
AMF node settings	206
AMF N2 interface settings	210
UPF Ranges configuration settings	211
UPF N3 interface settings	212
MME Ranges configuration settings	213
MME node settings	214
MME S1 interface settings	216
SGW Ranges configuration settings	217
SGW S1-u interface settings	218
SEG Ranges configuration settings	219
SEG interface settings	223
N3IWF Ranges configuration settings	224
N3IWF interface settings	230
Chapter 7 Manage and use test sessions	236
Save test sessions	236
Manage test sessions	237
Import and export sessions	239
Delete configs and sessions	240
Chapter 8 Manage CoreSIM licenses	242
Licensing Requirements	242
License Manager	242
License Server	244
Chapter 9 Manage CoreSIM users	246
Chapter 10 CoreSIM general settings	250
Chapter 10 Statistics	252
Chapter 11 Troubleshooting	254
View Notifications and Test Events	254
Collect Diagnostics, Cleanup and Data Migration	256
NTP troubleshooting	259
Appendix A Predefined Applications	A

Appendix B Application Actions O

Index BS

CHAPTER 1

Introduction

A 4G/5G core simulator, CoreSIM makes Radio Access Network testing easier by eliminating Core Network unwanted dependencies and allowing an easily controllable, repeatable test environment setup. RAN test efforts can thus be concentrated on the Device Under Test, speeding up 3GPP standards implementation.

Highly scalable, CoreSIM allows up to hundred independent test lines in parallel.

Objectives-based testing

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

UI overview

The Keysight CoreSIM 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 Keysight Open RAN Simulators, Cloud Edition 2.0 instance.

The major elements of the UI are:

- [Application framework elements below](#)
- [Dashboard page on the next page](#)
- [Test overview page on the next page](#)
- [Configuration properties pages on the next page](#)
- [Statistics page on the next page](#)

Application framework elements

CoreSIM uses a web-based UI that is common to a number of Keysight applications, including LoadCore and CyPerf. The web page framework includes the following elements:

Title bar

The title bar, which is located across the top of the Keysight Open RAN Simulators, Cloud Edition 2.0 window, is present on all pages, and provides key information and controls, including:

- Keysight logo: Click the Keysight logo from any point in the interface to return to the dashboard page.

- Session identifier: Shows the current session number and test config name. Clicking the session identifier returns you to the TEST OVERVIEW page.
- Events menu (🔔): Provides access to notifications and test events.
- Links to the OVERVIEW and STATISTICS pages.
- User profile menu: The user profile menu provides access to the current user's Edit Account screen in which you can edit your profile preferences, switch theme and logout.
- Settings menu (⚙️): Provides access to a number of application and administrative functions and resources, including user Logout, License Manager, Agent Management, software update, diagnostics (test logs), product information, and more.

Tool bar

The tool bar is located directly under the title bar. It provides access to functions and content that are specific to your current application context. The **START TEST** and **STOP TEST** buttons are located on the tool bar.

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 CoreSIM 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.

Test overview page

When you create a test session based on any predefined, newly-created, or imported test configuration, CoreSIM opens the **TEST OVERVIEW** page on which you can view a summary of the test configuration and a visual representation of the test topology. The Overview includes a test progress bar, timeline and objectives summary data, a link to the Global Settings, and the test topology section.

The test topology is an interactive graphical representation of the test network. From the topology, you access all of the configurable elements for the current test.

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.

CoreSIM 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.

Additional information and resources

All of the information in this User Guide is based on the assumption that CoreSIM has already been successfully deployed in your network. The following resources provides information that is not covered in this guide:

Resource	Location
Software and documentation download page	Downloads & Updates
<i>KORA Deployment Guide</i>	A copy is available on the Software Downloads page cited above.
Keycloak user documentation	https://www.keycloak.org/documentation

This page intentionally left blank.

CHAPTER 2

Initial administrator login

This chapter describes the actions that are required the first time you log in to CoreSIM 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 the next page](#)

Required information

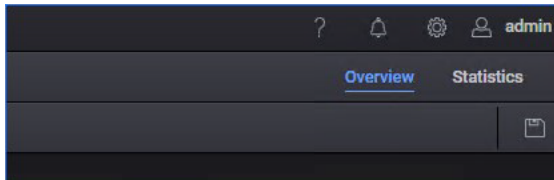
- The IP address that you set for the CoreSIM web interface during deployment.
- The IP address of the license server.
The license server is shipped as a separate `.ova` file. After deploying the `.ova` file, you can access it using a web browser.
- Your CoreSIM license activation codes (or entitlement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

Initial login and password change

CoreSIM 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 CoreSIM instance in your browser's address field. CoreSIM 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, CoreSIM 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 CoreSIM title bar.



CoreSIM 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 CoreSIM deployment.

To activate your licenses:

1. Select **Administration** from the setup menu (⚙️).
2. Select **License Manager** from the **Administration** menu. CoreSIM opens the **License Manager** page.
3. To activate your licenses:
 - a. Select **Activate licenses**.
CoreSIM 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 (⚙️).
CoreSIM opens the **Application Settings** dialog.
2. Select your **License Provider** from the drop-down list:
 - **Legacy License Server** - this option is set by default on CoreSIM (using the old LicenseManager).
 - **External License Server** - select this option to set an external license server (using the new LicenseManager 1.7).
 - **Embedded License Server** - the license server that is included in the middleware.
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). Further, it is recommended that you use the admin account only for administrative activities.

Refer to [Manage CoreSIM users](#) for detailed information about user account management.

This page intentionally left blank.

CHAPTER 3

User login and logout

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

Log in as a regular user

The user accounts that the CoreSIM 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 CoreSIM IP address in your browser's URL address field.
2. Press **Enter** to access the Keysight**Login** window.
3. Enter your 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, CoreSIM opens the dashboard.

Log out

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

This page intentionally left blank.

CHAPTER 4

Build and run a test

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

Chapter contents:

Create a new test config	20
Configure the test	21
Start the test	22
View real-time test results	23
Test results	23

Create a new test config

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

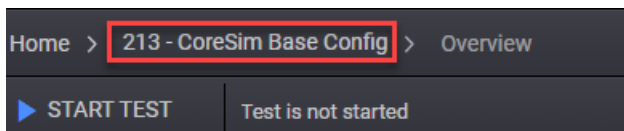
- [Create a config based on a template below](#)
- [Create a new config based on an existing config on the next page](#)

Create a config based on a template

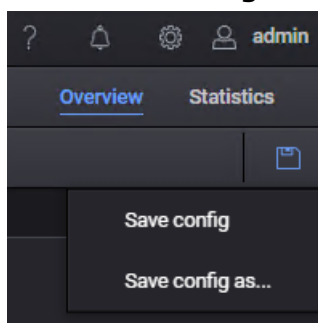
1. Log in to CoreSIM.
2. In the Dashboard page, select the **Wireless CoreSIM** template from the **Create New Test** panel.

CoreSIM opens the **Test Overview** page, which includes the graphical representation of the test topology.

CoreSIM 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...**



CoreSIM 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.

Create a new config based on an existing config

Rather than creating a new config based on one of the CoreSIM 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.

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 template. In effect, you can create private templates that are pre-populated with configuration values that you will typically use in your testing.

Configure the test

To configure this test, do the following:

1. On the CoreSIM Dashboard page, under the Create New Test section, select **Wireless CoreSim**.
The Test Scenario page appears.
2. On the Test Overview panel configure Global Settings. These settings become immediately available for selection in several of the node configuration windows. You define them once and reuse them multiple times.
For more details about Global Settings configuration, refer to [Global Settings panel](#).
3. Select the services and nodes that the CoreSIM will simulate. Select any or all of the other (non-DUT) nodes and services for testing (they are all selected by default, so you can simply deselect any that you do not require for a test). CoreSIM will simulate these elements during testing.
4. Configure the test settings for the simulated nodes and services. You can configure the nodes in any order, but it may be helpful to work outwards from the DUTs.
You can click on a node, select one of the ranges (this is a per-range option) and by enabling the **Device Under Test** option, that node will no longer be simulated by our CoreSIM. You still need to configure the IP addresses of the DUT so the nodes simulated by CoreSIM know who they need to communicate with.
For each node configuration, refer to its dedicated section, as follows:
 - [SEG & CoreSim](#)
 - Data Networks (DN)
 - IP Multimedia Subsystem (IMS)
 - Radio Access Network (RAN)
5. Select the number of traffic agents for each CoreSIM node. For more details, refer to [Traffic Agents](#).
6. Configure the test settings for the simulated UEs. While there are a large number of UE configuration settings, you can often use the default values with little or no modification.
For UE configuration, refer to [User Equipment \(UE\)](#).
7. On the [User Equipment \(UE\)](#), configure the test objectives.

The test *Objectives* determine the behavior of the simulated UEs. The User Plane Objectives determine the volume and rate of data traffic, and The Control Plane Objectives determine the volume and rate of control plane procedures.

8. Start the test. When you click or tap the **Start Test** button, CoreSIM begins the registration procedure, any other configuring or occurring control plane procedure and traffic generation. For more details, refer to [Start the test](#).

9. Evaluate the results.

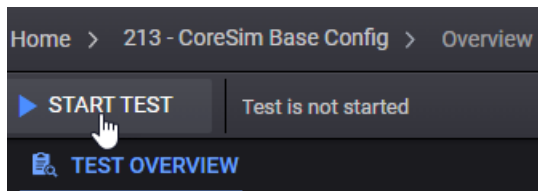
Once the test is running, you can click or tap **Statistics** to start monitoring the progress of the test.

TIP

If there are multiple test sessions, you can quickly switch between them by selecting the small green triangle next to the name of the current test session. A drop-down list will displays all your current test sessions and allows you to change to a specific test session by selecting it.

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 CoreSIM tool bar displays the test status throughout its execution progress. In addition, each test session tile (located on the CoreSIM 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.

CoreSIM 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, CoreSIM 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.

View real-time test results

When you successfully start a test, CoreSIM immediately displays the [STATISTICS](#) page, where you can view real time statistics.

Test results

The Browse Results section can be accessed in order to retrieve the test results, packet captures and logs, and export them.

To access the Test Results window, select **Browse Results**.

The Test Results window displays details about each test that was previously ran regarding the name and the test configuration, the status and the start time of the test, along with the test duration and the user that initiated the test.

On this section, the following actions are possible:

- Search for the results of a specific test.
- Load the test configuration in a new session, by selecting the **Load** button.
- Download the test results and packet captures, by selecting **Download**:
 - **CSV** - download the test results as a CSV.
 - **Report** - download the test results as a pdf file.
 - **Captures** - download an archive containing both MW and Agent logs.

NOTE

To download the captures you need to enable traffic capture on the test agents.

- **Config**
- **Test Diagnostics**
- Delete the test results, by selecting the **Delete** button.

CHAPTER 5

Assign and manage agents

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

Chapter contents:

About traffic agents	24
Assigning agents to nodes	24
Agent management	25
Network Management	28

About traffic agents

CoreSIM tests require the use of *agents* to generate traffic for both UP (user plane) and 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.


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 CoreSIM. 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 the next page for instructions.

Assigning agents to nodes

You cannot run a CoreSIM 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.
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.

CoreSIM 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.

Agent Assignments window

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

Column	Description
Owner	<p>Hover over the Owner icon to see the current agent ownership and status, which will be one of the following:</p> <ul style="list-style-type: none"> • The agent is owned by the user whose email address is listed. In this case, the agent is not available for assignment. • The agent is offline. In this case, the agent is not available for assignment. • The agent is available for assignment.
Select Agent	<p>Use the check box next to the IP address to select that agent for assignment. You can also select all available agents by selecting the Select Agent check box (in the table header).</p>
Tags	<p>This column displays the tags associated with each agent. Each tag indicates the number of agents to which it is associated.</p> <p>Refer to About traffic agents for more information about tags.</p>
Connections	<p>The table displays the available interface and the MAC address for each wireless connection. The interface can be selected from the drop-down list.</p> <div style="display: flex; align-items: center;"> <div style="background-color: #d3d3d3; padding: 2px 5px; margin-right: 10px;">NOTE</div> <p>For the CoreSIM nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.</p> </div>

Agent management

You manage your CoreSIM 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 on the facing page](#)
- [Selecting agents on the facing page](#)
- [Search, select, and filter agent data on page 27](#)
- [Adding and removing tags on page 27](#)
- [Agent management actions on page 27](#)

Agent Management window

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

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

Selecting agents

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

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

Search, select, and filter agent data

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

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

Adding and removing tags

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

Add a custom tag:

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

Remove a tag:

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

Agent management actions

You can perform the following actions on the agents that are currently selected (selected via the selection check box 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).

Function	Description
Soft reboot	Performs a soft reboot on the agent (the agent system restarts without a power cycle).
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.
Impairment profile	Allows you to select an impairment profile from the drop-down list.
Agent Interface	Displays the agent's interface Name and MAC address.
Network Stack	<p>This option allows you to select the network stack used to run the test:</p> <ul style="list-style-type: none"> • Linux Stack • IxStack over Raw Sockets • IxStack over DPDK <p>An agent compatible with IxStack is marked using an IxStack: On/Off system tag.</p>
SRIoV	This option is disabled when <i>Network Stack</i> is set to Linux Stack. For IxStack over Raw Sockets or IxStack over DPDK, this option is enabled based on the selection (it can be enabled or disabled based on your agent's configuration).
Traffic Capture	<p>This option allows you to enable or disable traffic capture on all or specific interfaces, based on your test configuration. This option can be used while a test is running.</p> <p>If the test was started with the capture disabled, you can enable the capture</p>

Column	Description
	<p>during the test. After enabling the capture, you must select Apply for the changes to take effect. The capture can be downloaded using the Download Capture button. To stop the capture, you must disable the traffic capture (using the toggle button) and then select Apply.</p> <p>Also, if the test was started with the traffic capture enabled, the capture can be stopped while the test is running.</p>
Download Capture	Select to download the traffic capture.
Entity	Displays the nodes on which the agent has been assigned. When hovering over the node, it displays the node's interface names.

IMPORTANT

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

Filtering agents

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

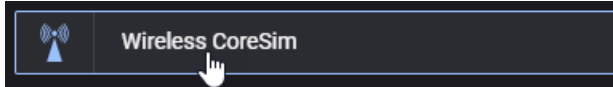
1. Select **Filter agents**.
2. Enter the name of the tag or select it from the available list.
3. Select **Close**.

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

CHAPTER 6

CoreSim tests: configuration settings

This section provides descriptions of the configuration settings that are specific to the **Wireless CoreSim** test type:



A 5G core simulator, CoreSim makes Radio Access Network testing easier by eliminating Core Network unwanted dependencies and allowing an easily controllable, repeatable test environment setup. RAN test efforts can thus be concentrated on the Device Under Test, speeding up 3GPP standards implementations.

Topics:

Global Settings	33
Global Settings panel	36
Node Start/Stop Rates	36
DNS Settings	37
Advanced Settings	37
DNNs panel	40
DNN configuration settings	40
Session AMBR configuration settings	44
ePCO configuration settings	44
Traffic Control Settings configuration	46
Impairment	47
QoS Flows panel	48
QoS Flow configuration settings	48
QoS Flow Packet Filter configuration settings	51
QoS Flow Max Packet Loss Rate settings	53
QoS Flow ARP configuration settings	53
QoS Flow MBR configuration settings	54
QoS Flow GBR configuration settings	54
Milenage	54
Customer Parameters	55
CA Certificates	55
UE configuration settings	56

UE Ranges panel	56
UE Range panel	57
Range Settings	58
UE Identification settings	59
UE Security settings	60
UE Settings settings	63
UE Subscribed AMBR settings	70
DNNs Config	70
SMS Configuration	73
Untrusted WiFi Settings	73
Network Slicing settings	75
UE NSSAI settings	76
UDM SNSSAI Mappings	77
Objectives	77
Control Plane Objective	78
About primary objectives	78
Primary Control Plane Objective	80
Secondary Control Plane Objective	82
Handover	83
Paging	85
Enter/Exit Idle	86
Create/Delete QoS Flows	87
Create/Delete PDU Sessions	89
SMS	90
User Plane Objectives	91
Stateless UDP Traffic	92
Data Traffic	94
Voice Traffic	98
Video OTT Traffic	113
DNS Client Traffic	116
ICMP Client	119
Capture Replay	120

Synthetic	122
UDG	124
Predefined Applications Traffic	128
Applications	130
Application Advanced Settings	133
TCP Settings	135
TLS Settings	136
RTP Settings	138
DN configuration settings	138
DN Ranges panel	139
DN Range panel	139
DN N6 interface settings	140
DN routes settings	141
DN User Plane	142
DN Stateless UDP Traffic	143
DN Data Traffic	144
DN Voice Traffic	147
DN Video OTT Traffic	158
DN DNS Server Traffic	161
DN Predefined Applications Traffic	163
DN Capture Replay	164
DN Synthetic	166
DN UDG	168
IMS configuration settings	170
CSCF Range panel	170
Media Function Range panel	171
RAN/Untrusted AP configuration settings	171
gNodeB	172
gNodeB Ranges panel	173
gNodeB Range settings	176
gNodeB node settings	177
gNodeB NSSAI settings	180

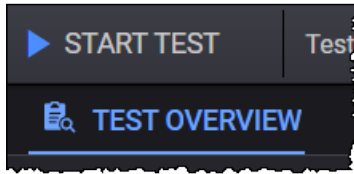
gNodeB N2 interface settings	181
gNodeB N3 interface settings	185
eNodeB	189
eNodeB Ranges panel	189
eNodeB Range Settings	193
eNodeB Node Settings	194
S1-U Interface Settings	195
S1-MME Interface Settings	196
UNAP	198
UNAP Ranges panel	198
UNAP Range Settings	199
Passthrough interface settings	200
SEG/N3IWF & CoreSim configuration settings	202
Core settings	203
N6/SGi interface settings	203
AMF Ranges configuration settings	205
AMF node settings	206
AMF N2 interface settings	210
UPF Ranges configuration settings	211
UPF N3 interface settings	212
MME Ranges configuration settings	213
MME node settings	214
MME S1 interface settings	216
SGW Ranges configuration settings	217
SGW S1-u interface settings	218
SEG Ranges configuration settings	219
SEG interface settings	223
N3IWF Ranges configuration settings	224
N3IWF interface settings	230

Global Settings

The 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 **Test Overview** tab:

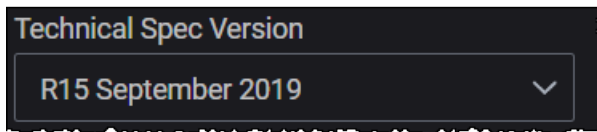


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



CoreSIM opens the **Global Settings** panel from which you can:

- Select the technical specification version from the drop-down list:



- Access and configure the following settings:

Global Settings panel	36
Node Start/Stop Rates	36
DNS Settings	37
Advanced Settings	37
DNNs panel	40
DNN configuration settings	40
Session AMBR configuration settings	44
ePCO configuration settings	44
Traffic Control Settings configuration	46
Impairment	47
QoS Flows panel	48
QoS Flow configuration settings	48
QoS Flow Packet Filter configuration settings	51
QoS Flow Max Packet Loss Rate settings	53
QoS Flow ARP configuration settings	53
QoS Flow MBR configuration settings	54
QoS Flow GBR configuration settings	54

Milenage54

Customer Parameters 55

CA Certificates55

Global Settings panel



When you open the Global Settings for editing (from the **Test Overview** section), CoreSIM opens the **Global Settings** panel. That panel provides a set of global configuration settings and links to more detailed settings.

Configuration settings

The following table describes the settings that are available on the Global Settings panel.

Setting	Description
<i>Links to detailed settings:</i>	
Node Start/Stop Rates	For more details, refer to Node Start/Stop Rates .
DNS Settings	For more details, refer to DNS Settings .
Advanced Settings	For more details, refer to Advanced Settings .
DNNs	For more details, refer to DNNs .
Impairment	For more details, refer to Impairment .
QoS Flows	For more details, refer to QoS Flows .
Milenage	For more details, refer to Milenage .
Custom Parameters	For more details, refer to Custom Parameters .
CA Certificates	For more details, refer to CA Certificates .

Node Start/Stop Rates



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

Setting	Description
<i>Node Start</i>	
Rate	Set the desired start rate for SCTP connections between the NG-RAN and the AMF (connections per second). Measured in procedures per second if Distributed over (s) is not modified.
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.

Setting	Description
<i>Node Stop</i>	
Rate	Set the desired start rate for SCTP connections between the NG-RAN and the AMF (connections per second). Measured in procedures per second if Distributed over (s) is not modified.
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.

DNS Settings

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

Setting	Description
<i>DNS Settings:</i>	
Cache Timeout (ms)	The amount of time (in milliseconds) the local DNS stores the address information.
<i>DNS Name Servers:</i>	
	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 following table describes the settings required to enable user plane and control plane advanced statistics.

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.

Setting	Description
Enable Capture On Loopback Interface	Select this option to enable packet capture on the loopback interface.
Enable Per UE Stats	Select this option to enable per UE statistics.
Enable QoE Stats	Select this option to enable per QoE statistics. This includes both PDU and QoS views.
Enable Control Plane Advanced Stats	Select this option to enable control plane latency statistics.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: <ul style="list-style-type: none"> • None - no advanced statistics enabled. • One Way Delay - the time spent by the packet on the network from the moment it is sent until it is received. • Delay Variation Jitter - the per polling interval average delay variation jitter value calculated for all packets.
Automated Polling Interval	This option is enabled by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval (sec)	This option becomes available only when <i>Automated Polling Interval</i> option is disabled. It allows you to create a custom polling interval.
Log Level	Select one of the options: <ul style="list-style-type: none"> • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful 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.
Traffic Settings	The settings are described here .

Setting	Description
Response Cache Settings	The settings are described here .
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.

Traffic Settings

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

Setting	Description
<i>GTPU Source Port:</i>	
Start	Indicates the source port for the GTPU tunnel. By default, the registered UDP port for GTPU is 2152.
Count	Set the count value.
<i>Reserved cores for RTP Tx:</i>	
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.
<i>Traffic Control</i>	
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.

Response Cache Settings

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

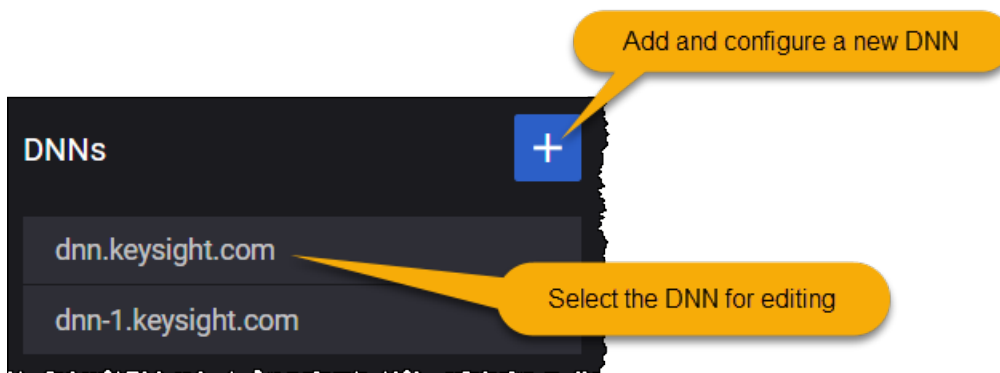
A rotation interval higher than the retry timer on the client node must be configured in order to still have the responses stored when a message retry arrives on the server node.

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

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

DNNs panel

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



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

DNN configuration settings	40
Session AMBR configuration settings	44
ePCO configuration settings	44
Traffic Control Settings configuration	46

DNN configuration settings

You create and manage Data Network Names (DNNs) for your test network in the **Global Settings** section of the **Test Overview**. The **DNN** panel contains the configuration settings for an individual DNN. In this panel, you can:

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

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

Setting	Description
<i>DNN:</i>	
DNN	Enter the DNN value for this DNN definition. For example: dnn.keysight.com.

Setting	Description
	<p>A DNN (as is the case with an EPS APN) is composed of two parts:</p> <ul style="list-style-type: none"> • A mandatory Network Identifier that defines the external network to which the UPF is connected. • An optional Operator Identifier that defines the PLMN backbone in which the UPF is located. <p>A 5GS Data Network Name (DNN) is equivalent to an EPS APN. It is a reference to a data network, and it may be used to select an SMF or UPF for a PDU session and to determine policies applicable to the PDU session.</p> <p>The DNN field supports dynamic values. These values can be obtained with a sequence generator.</p> <p>The sequence can be added anywhere in the DNN name (beginning, middle or end). The syntax is <code>[start_value-end_value,increment]</code>.</p> <div style="display: flex; align-items: flex-start;"> <div style="background-color: #cccccc; padding: 5px; margin-right: 10px; text-align: center;">NOTE</div> <div> <p>The <code>start_value</code> and <code>end_value</code> must have the same length. For example, we can configure <code>dnn[008-999,1]</code> and obtain <code>dnn008</code>, <code>dnn009</code>, ..., <code>dnn998</code>, <code>dnn999</code>. Syntaxes <code>dnn[8-999,1]</code> or <code>[008-1000,1]</code> are not valid as the start and end value lengths are different.</p> </div> </div> <p>The start value is mandatory. Omitting certain parameters results in behaviors as exemplified below:</p> <ul style="list-style-type: none"> • <code>dnn[4-9,]</code> an implicit increment of 1 is used • <code>dnn[4-9]</code> as above • <code>dnn[4-,1]</code> is used as <code>dnn[4-9,1]</code>, 9 being the maximum value with the configured length, length of 1 in this case • <code>dnn[4-,]</code> as above • <code>dnn[4-]</code> as above • <code>dnn[4]</code> as above <p>UEs will use the DNN values from the pool in a round robin manner.</p> <div style="display: flex; align-items: flex-start;"> <div style="background-color: #005596; color: white; padding: 5px; margin-right: 10px; text-align: center;">IMPORTANT</div> <div> <p>If multiple sequence generators are configured and their pools overlap (for example: <code>dnn[000-600,1].keysight.com</code> <code>dnn[500-999,1].keysight.com</code>), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the <code>start_value</code> (they might start with an intermediate value in the second pool).</p> </div> </div>
PDU Type	Select the desired PDU type: IPv4, IPv6 or IPv4v6.
Allowed Session Types	Select the allowed session types from the drop-down list: IPv4 IPv6, IPv4, IPv6, UNSTRUCTURED, ETHERNET, or all.
Default Session Type	Select the default session type from the drop-down list: IPv4 IPv6, IPv4, IPv6, UNSTRUCTURED, or ETHERNET.

Setting	Description
QoS Flows IDs	<p>Select the QoS Flows ID(s) from the drop-down list. Each DNN should contain at least the default flow (the default flow is unique per each DNN). In addition, zero or more dedicated flows can be associated to each DNN.</p> <p>For more details about QoS Flow configuration, refer to QoS Flow configuration settings.</p>
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> • SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. • SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) that had been allocated to the UE. • SSC Mode 3: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Default SSC Mode	<p>Select the desired default SSC mode for this DNN.</p> <p>The SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session.</p>
Allowed Services	<p>Select the allowed services from the drop-down list: Service 1, Service 2, Service 3, or all. In the 5G System, the <i>allowed services</i> may comprise any number of service identifiers allowed for the subscriber in the PDU Session. The PCF maps those service identifiers into PCC rules according to local configuration and operator policies.</p>
Subscription Categories	<p>Select the desired Subscription Category for this range of UEs.</p> <p>Subscriber Category is an information type structured as a list of category identifiers associated with a subscriber. It may comprise any number of identifiers associated with the subscriber (such as platinum, gold, silver, bronze).</p>
IPv4 Index	<p>The IPv4 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv4 addresses.</p>
IPv6 Index	<p>The IPv6 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv6 addresses.</p>
EPS Interworking	<p>Enable this option if the UE subscription data indicates support for interworking with EPS for this DNN.</p>
ADC Support	<p>Enable this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.</p>

Setting	Description
Subscriber Spending Limits	Enable this option if the DNN will support PDU session policies that are based on subscriber spending limits.
Offline	Enable this option if the DNN will support the offline charging method for PDUs sessions.
Online	Enable this option if the DNN will support the online charging method for PDUs sessions.
Is Emergency DNN	When this option is enabled, if an UE range has mapped this type of DNN, it will perform an emergency PDU Session.
MPS Priority	Enable this option if the DNN will support subscription to MPS priority service. The priority applies to all traffic on the PDU Session.
Dual Registration Mode	When enabled, it transfers this session to the other RAT in dual registration mode. If the session does not exist, it will be created in the other RAT.
MPS Priority Level	Specify the Multimedia Priority Services (MPS) priority level. This is the relative priority level for MPS.
IMS Signaling Priority	Specify the IP Multimedia Subsystem (IMS) signaling priority. This value indicates subscription to IMS signaling priority service. The priority applies only to IMS signaling traffic.
Access Network Instance	Set the access network instance. It represents the value to be sent in the Network Instance IE when the source interface is set to Access.
Core Network Instance	Set the core network instance. It represents the value to be sent in the Network Instance IE when the source interface is set to Core or SGI-LAN/N6-LAN.
Session Rule Name	Set the session rule name.
<i>GBR</i>	<i>Select this option to open the GBR panel.</i>
Guaranteed Bit Rate Uplink	Specify the guaranteed bit rate for the uplink traffic.
Guaranteed Bit Rate Downlink	Specify the guaranteed bit rate for the downlink traffic.
<i>Session AMBR</i>	<i>Select this option to open a new panel that contains the Session AMBR settings. These settings are described in Session AMBR configuration settings.</i>

Setting	Description
ePCO	Select this option to open the extended protocol configuration options panel. These settings are described in ePCO configuration settings .
Traffic Control Settings	Select this option to open the traffic control settings panel. These settings are described in Traffic Control Settings configuration .

If, for an UE range, Paging is configured and globally per DNN Traffic Control is configured, for that UE range traffic control messages will be sent before entering Idle (as per the Paging objective) but traffic control messages will be sent per DNN as configured in the **Global Settings > DNN > Remote IPv4/IPv6** and traffic will be resumed per DNN as configured in the **Global Settings > DNN > Suspend Traffic Interval (s)** field.

Session AMBR configuration settings

Each CoreSIM DNN configuration has its own unique configuration settings, which include:

- The main DNN settings, described in [DNN configuration settings](#).
- The DNN's Session AMBR settings, described below.

About Session AMBR ...

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

The following tables describes the Session AMBR configuration settings.

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

ePCO configuration settings

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

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

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

Known limitations:

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





Traffic Control Settings configuration

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

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



The following tables describes the Traffic Control Settings parameters.

Parameter	Description
Traffic Control Settings	By default, this option is disabled. Select the check box to enable it.

Parameter	Description
Suspend Traffic Interval(s)	Set the value (in seconds) for this parameter.
Delay Between PDU Session Establishment and Suspend Traffic	Set the value (in seconds) for this parameter.
Remote IPv4	Select: <ul style="list-style-type: none">  - Select to add the remote IPv4 address.  - Select to remove the remote IPv4 address.
Remote IPv6	Select: <ul style="list-style-type: none">  - Select to add the remote IPv6 address.  - Select to remove the remote IPv6 address.

Impairment

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

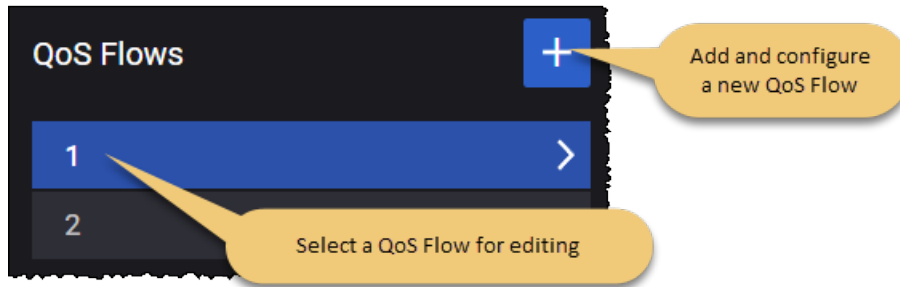
Setting	Description
<i>Impairment Profiles:</i>	
	Select the Add impairment profile button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the Delete impairment profile button to remove the profile from your test configuration.
Name	Each impairment profile is uniquely identified by a name. You can accept the value provided by CoreSIM 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.

QoS Flows panel

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

Accessing the configuration settings:

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



q

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

QoS Flow configuration settings	48
QoS Flow Packet Filter configuration settings	51
QoS Flow Max Packet Loss Rate settings	53
QoS Flow ARP configuration settings	53
QoS Flow MBR configuration settings	54
QoS Flow GBR configuration settings	54

QoS Flow configuration settings

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

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

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

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

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

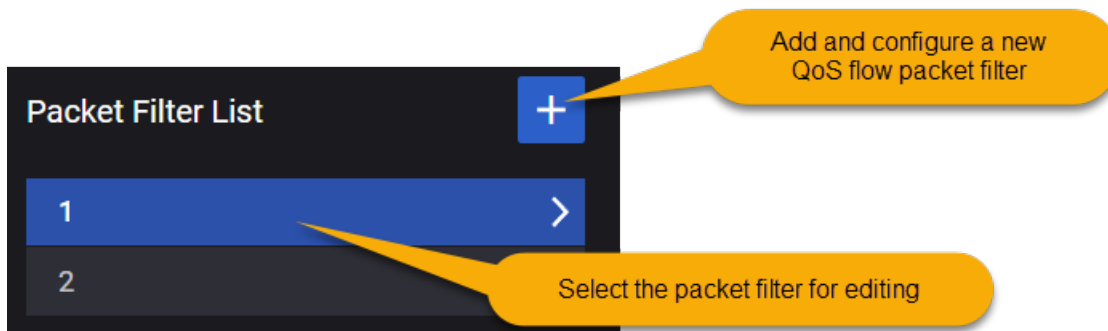
Setting	Description
QoS Rule Precedence	Specify the desired QoS Rule Precedence value for this QFI. The QoS rule precedence value (and the PDR precedence value) determine the order in which a QoS rule or a PDR, respectively, will be evaluated. The evaluation of the QoS rules or PDRs is performed in increasing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

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


QoS Flow Packet Filter configuration settings

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

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



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

Setting	Description
	Select the Delete Packet Filter button to delete this Packet Filter from the test configuration.
Direction	Select the direction of the data flow on which the filter is applied from the drop-down list: Uplink, Downlink, or Bidirectional.
IPv4 Remote Address and Subnet Mask	The IPv4 address of the remote node plus the subnet mask. If the <i>Direction</i> is Uplink, then this IP address is the destination IP. If the <i>Direction</i> is Downlink, then this IP address is the source IP.
IPv6 Remote Address and Prefix Length	The IPv6 address for the remote node, expressed in CIDR notation (for example: 2001:db8::/32). If the <i>Direction</i> is Uplink, then this IP address is the destination IP. If the <i>Direction</i> is Downlink, then this IP address is the source IP.
Protocol Identifier or Next Header	The Protocol ID of either the protocol above IP in the stack or the next header type. Examples: UDP, TCP, ESP.
Single Local Port	The local port number, if the filter specifies a single port.
Single Remote Port	The remote port number, if the filter specifies a single port.
Local Port Range	The low and high limits for local port range.
Remote Port Range	The low and high limits for remote port range.
Security Parameter Index	The Security Parameters Index (SPI) for this packet filter. The SPI is a pointer that references the session key and algorithms used to protect the data being transported.
Type Of Service or Traffic Class	The IPv4 Type of Service (TOS) or the IPv6 traffic class.
Flow Label	The IPv6 Flow Label. This refers to the 20-bit Flow Label field in the IPv6 header.

QoS Flow Max Packet Loss Rate settings

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

Setting	Description
<i>5G QoS Flow, Maximum Packet Loss Rate:</i>	
Uplink	The maximum uplink packet loss rate (packets per second) that is permitted for the QoS Flow.
Downlink	The maximum downlink packet loss rate (packets per second) that is permitted for the QoS Flow.

QoS Flow ARP configuration settings

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

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

Setting	Description
<i>5G QoS Flow, ARP:</i>	
ARP Priority Level	Specify the ARP priority level. The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.
Preemption Capability	Enable this option if the packets in this QoS Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.
Preemption Vulnerability	Enable this option if the packets in this QoS Flow are candidates for being preempted by other flows. When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.

QoS Flow MBR configuration settings

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

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

Setting	Description
5G QoS Flow, MBR:	
Uplink Bitrate Unit	Select the uplink bitrate unit from the drop-down list.
Uplink Bitrate Value	Set the maximum bit rate value for uplink traffic.
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set the maximum bit rate value for downlink traffic.

QoS Flow GBR configuration settings

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

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

Setting	Description
<i>5G QoS Flow, GBR:</i>	
Uplink Bitrate Unit	Select the uplink bitrate unit from the drop-down list.
Uplink Bitrate Value	Set the guaranteed bit rate value for uplink traffic.
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set the guaranteed bit rate value for downlink traffic.

Milenage

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

Setting	Description
<i>Milenage Constants</i>	
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.

Setting	Description
Name	Each certificate is uniquely identified by a name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Certificate File (.crt)	It allows you to add the certificate from the storage location, using the Upload button. To remove the script, select the Clear button.

UE configuration settings



You use the User Equipment (UE) configuration settings to define one or more ranges of simulated UEs. Every test requires at least one range of simulated UEs. These settings define properties that are representative of real-world UEs that may access a 5G network, including UE identity, security, network slice selection, among others.

In addition, the UE settings include the configuration of test objectives; these settings direct the traffic performance and UE behavior actions during test execution.

The configuration settings are described in the topics listed below.

Topics:

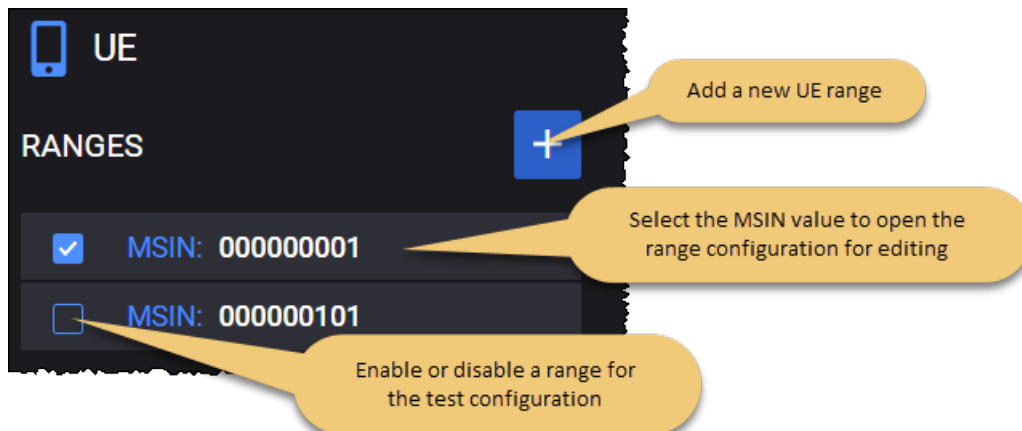
UE Ranges panel	56
UE Range panel	57
Range Settings	58
UE Identification settings	59
UE Security settings	60
UE Settings settings	63
UE Subscribed AMBR settings	70
DNNs Config	70
SMS Configuration	73
Untrusted WiFi Settings	73
Network Slicing settings	75
UE NSSAI settings	76
UDM SNSSAI Mappings	77

UE Ranges panel

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

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

For example ...



UE Range panel

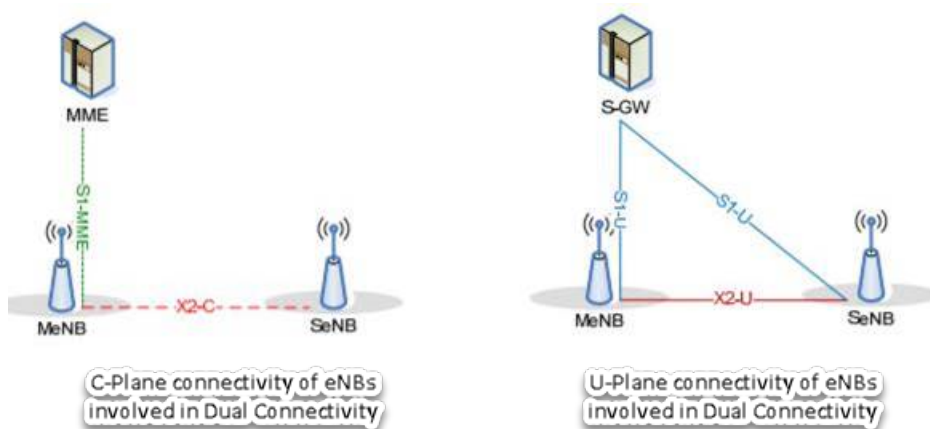
When you select an MSIN from the UE **Ranges** panel, CoreSIM opens the **Range** panel, from which you can:

- Delete the UE range from the test configuration.
- Configure the *Range Count*.
- Create copies of your range by providing the number of copies and selecting the **Create Range Copies** button.
- Select the *Parent NG-RAN/UNAP* for the UE range.
- Select a *Secondary Node*.
- Access the detailed UE configuration settings (Range Settings, Network Slicing, Objectives).

UE range controls and settings

CoreSIM has now support for Option 3x, on the NG-RAN, simulating Dual Connectivity radio connections, as described in 3GPP TS 36.300/38.300.

This will enable the UEs to use the radio resources for sending/receiving application traffic on both E-UTRAN and NR, as seen in the following topology.



The eNodeBs and gNodeBs involved in the communication must have a X2 connection established between them.

The eNodeBs/gNodeBs involved in this communication will have two optional roles:

- a Parent Node – (only eNodeB at this point), or
- a Secondary Node (a gNodeB).

The UE will attach to a 4G eNodeB which can have a Secondary node configured, a gNodeB. This implies all the traffic or just a part of it can be sent through the NR bearer, the IP and GTP tunnel being negotiated in the E-RAB modification procedure over the S1 interface.

Through E-RAB modification CoreSIM supports the following:

- SN addition
- SN change
- SN modification
- SN release


Since the UEs will be able to use both E-UTRAN and NR resources, not all the established bearers need to be moved.

In this configuration, the **Move to Secondary Node** option must be enabled on the QoS flows tab, on each bearer that needs to use the NR resources. The traffic will be moved to NR bearers as soon as the bearer configured to support is successfully setup.

Known limitations:

- Application Traffic is not supported on Dual Connectivity bearers.

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Range Count	Enter the number of simulated UEs required for the range.
Parent RAN/UNAP	Select the desired parent node from the test configuration. This will be the NG-RAN through which the UEs in the range will access the 5G core network.
Secondary Node	This option is used for Option 3x and Dual Connectivity NR-NR features. Select the secondary node from the drop-down list.

Range Settings

For each range that you add (in the [UE Ranges panel](#)), you configure the settings from the **Range** panel ([UE Range panel](#)).

The **Range Settings** are organized into the following groups:

UE Identification settings	59
UE Security settings	60
UE Settings settings	63
UE Subscribed AMBR settings	70
DNNs Config	70
SMS Configuration	73
Untrusted WiFi Settings	73

UE Identification settings

Each UE range has a set of Identification settings that provide basic identity values for the simulated UEs that populate the range. Some of the values (such as MCC) are shared by all of the UEs in the range, while others (such as MSIN) are unique for each individual UE in the range. The unique values are generated using an initial value plus an increment value.

The following table describes the UE **Identification Settings**.

Setting	Description
PLMN MCC	The MCC that will be assigned to each UE in this range.
PLMN MNC	The MNC that will be assigned to each UE in this range.
MSIN	The MSIN value that will be assigned to the first simulated UE in the range.
MSIN increment	The value to use for incrementing the MSIN values for each of the UEs in the range.
IMEI	The IMEI value that will be assigned to the first simulated UE in the range. The International Mobile Equipment Identity (IMEI) is a number used to uniquely identify 3GPP and iDEN mobile phones, as well as some satellite phones. It identifies the origin, model, and serial number of the device. It consists of either 15 digits (14 digits plus one check digit); or 16 digits (14 digits plus two software version digits). GSM networks use the IMEI number to identify valid devices, and can also use the number to prevent a stolen phone from accessing the network. When it includes the software version digits, it is referred to as the IMEISV.
IMEI Increment	The value to use for incrementing the IMEI values for each of the UEs in the range.
Software Version	The software version number identifies the software version number of the mobile equipment. Its length is 2 digits.
MSISDN	The first Mobile Station ISDN (MSISDN) value for this range.
MSISDN Increment	The value to use for incrementing the MSISDNs in the range.

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 deconceal 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 CoreSIM, 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 / OPc / TOP / TOPc	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 CoreSIM, 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 CoreSIM, 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.
TOP	A 256-bit operator variant algorithm configuration field used by the TUAK authentication algorithm.
TOPc	A 256-bit value derived from TOP and K used by the TUAK authentication algorithm.

Setting	Description												
TOPc Increment	The number used to increment the TOPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same TOPc value.												
SUCI Protection Scheme	The protection scheme used to generate the SUCI (for the purpose of concealing the SUPI) for each UE in the range. The options are as follows:												
	<table><tr><th>Scheme</th><th>Identifier</th><th>Size of the scheme output</th></tr><tr><td>null-scheme</td><td>0x0</td><td>Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)</td></tr><tr><td>Profile-A</td><td>0x1</td><td>Total of 256-bit public key, 64-bit MAC, and size of input</td></tr><tr><td>Profile-B</td><td>0x2</td><td>Total of 264-bit public key, 64-bit MAC, and size of input.</td></tr></table>	Scheme	Identifier	Size of the scheme output	null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)	Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input	Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.
	Scheme	Identifier	Size of the scheme output										
	null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)										
Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input											
Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.											
Home Network Public Key	The home network public key that will be use for concealing the SUPI. The USIM stores the home network public key (if provisioned by the home operator).												
Home Network Public Key ID	The Home Network Public Key Identifier that will be used to indicate which public/private key pair to use for SUPI protection and deconcealment of the SUCI.												
Ephemeral Public Key	The ephemeral public key that will be used for computing a fresh SUCI on the UE side and for deconcealing the SUCI on the home network side.												
Ephemeral Private Key	The ephemeral private key that will be used for computing a fresh SUCI on the UE side.												
Routing Indicator	<p>The Routing Indicator that is used in the construction of the SUCI.</p> <p>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.</p>												
RAND	<p>A hexadecimal number that represents the 128-bit random challenge.</p> <p>You can accept the value generated by CoreSIM, or enter of a RAND value of your own choosing.</p>												
RAND Increment	Specify the RAND increment value.												
AUTN	The AUthentication Token (AUTN) to use when authenticating the UEs in this range.												
Authentication Type	<p>Select the Authentication Method to use in the authentication procedures for this range of UEs.</p> <p>In the current release, 5G-AKA is the only supported Authentication Type.</p>												

Setting	Description
Integrity Protection Maximum Uplink Data Rate	Select a value from the drop-down list: <ul style="list-style-type: none"> • 64 kbps • Full Data Rate
Integrity Protection Maximum Downlink Data Rate	Select a value from the drop-down list: <ul style="list-style-type: none"> • 64 kbps • Full Data Rate

UDM User Plane Security Profile

The following parameters are required to configure the UDM User Plane Security Profile:

Parameter	Description
	Select the Add Security Profile button to add a new profile to your test configuration.
	Select the Delete Profile button to remove the profile from your test configuration.
UDM SNSSAI Mapping Profile	Select the mapping profile from the drop-down list.
DNNs	Select the DNN value for the drop-down list. For example: <code>dnn.keysight.com</code> .
Integrity	Select an option from the drop-down list: <ul style="list-style-type: none"> • REQUIRED • PREFERRED • NOT-NEEDED
Confidentiality	Select an option from the drop-down list: <ul style="list-style-type: none"> • REQUIRED • PREFERRED • NOT-NEEDED

When the **REQUIRED** option is selected for any of the [Integrity](#) or [Confidentiality](#) parameters and, on the NGRAN, the same option ([Enable Integrity](#) or [Enable Confidentiality](#)) is NOT selected, the NGRAN will send in *PduSessionResourceSetupResponse* message an error cause (forcing SMF to send a PDU Session establishment reject). Otherwise, for any other combinations of Integrity or Confidentiality parameters on UDM security profile and NGRAN, the flow should be successfully.

NOTE

User Plane Security settings are not taken into account for N2 Handover procedure.

UE Settings settings

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

Setting	Description
<i>Settings:</i>	
Dual Registration Mode	<p>When enabled, this option allows an UE to be registered/attached in the same time to 5GS via a gNodeB and to EPS via an eNodeB.</p> <p>The UE will activate this feature in case:</p> <ul style="list-style-type: none"> • Dual Registration Mode option is enabled. • At least one DNN has Dual Registration Mode option enabled. • It has a parent gNodeB (<i>gNodeB-1</i> for example). • It has a Handover objective configured with visited nodes (for example, primary node <i>gNodeB-1</i> and secondary node <i>eNodeB-1</i>). • the Core network advertise support for interworking without N26.
Allow MICO Mode	<p>This option, when selected, indicates that the UEs in the range prefer Mobile Initiated Connection Only (MICO) mode during Initial Registration and Registration Update procedures.</p> <p>Applicable to simulated UDM NF.</p>
Subscribed Registration Timer (s)	<p>The Periodic Registration timer value for this range of UEs.</p> <p>The AMF allocates a periodic registration timer value to the UE based on local policies, subscription information and information provided by the UE. After the expiry of this timer, the UE performs a periodic registration.</p> <p>Applicable to simulated UDM NF.</p>
Active Time (s)	<p>The subscribed Active Time for Power Saving Mode (PSM) UEs.</p>
RAT Restrictions	<p>UE Mobility Restrictions include RAT restrictions, which define the 3GPP Radio Access Technologies (one or more) that a UE is not allowed to access in a PLMN. The options available in CoreSIM are: NR, E-UTRA, WLAN, and Virtual.</p> <p>Applicable to simulated UDM NF.</p>
Set ESM Information Transfer Flag	<p>By default, this option is enabled.</p> <p>This option controls the value of the <i>ESM information transfer</i> flag from InitialUEMessage/AttachRequest 4G message.</p> <p>When this option is disabled, the UE/eNodeB will set the flag <i>ESM information transfer</i> to <i>False</i> and MME will not send DonwlinkNASTransport/ESM information request.</p>

Setting	Description
Switch Off Deregistration/Detach	When this option is enabled, the Deregistration Request/Detach messages will use a deregistration/detach type of Switch-off. When the Deregistration/Detach type is switch-off, the AMF/MME does not send the Deregistration/Detach Accept message back to the UE.
PDU Session Release Before Deregistration	When this option is enabled, the UE will release PDU sessions before deregistration.
Enable Periodic Registration Update	<p>By default, this option is not enabled.</p> <p>If the periodic registration functionality is disabled, the UE will ignore the T3512 timer received in the Registration Accept and will not send any Periodic Registration Update request.</p> <p>During the Initial Registration, the AMF sends in the Registration Accept a T3512 timer, which consists of a Unit-Value pair. For example, a value of 30 and unit of 10min means 300 minutes.</p> <p>The T3512 timer can be overridden by subsequent Registration Accept messages. If T3512 is 0 or Disabled, no periodic registration should be performed. If no T3512 value is present in the Registration Accept message, the last known T3512 value is used. If a T3512 was never transmitted by the AMF, the default value of 54 minutes will be used.</p> <p>The T3512 timer is triggered when the UE enters idle. If the UE exits the idle state, the T3512 timer is stopped. When the UE enters again in idle, the T3512 timer is restarted.</p> <p>While the UE is in idle mode, when the T3512 timer expires:</p> <ul style="list-style-type: none"> • If the UE is not registered for emergency services, the UE initiates a Periodic Registration Update procedure and restarts the T3512 timer. • If the UE is registered for emergency services, the UE locally de-registers and the AMF locally de-registers the UE.
Delay Before PDU Session Creation (ms)	The time that will elapse before the UEs in this range begin creating PDU sessions after successful Registration.
Delay Before Deregister (ms)	The time that will elapse between PDU Session Release Complete and UE initiated Deregistration Request messages.
Delay Before Handover Notify (ms)	The time to wait before handover notification.
Delay Before Paging (ms)	The time to wait before paging, after UE enters idle.
Paging Storm Iterations	The number of times the UE will be paged.
Paging Storm Interval (ms)	The delay between paging messages, in milliseconds.

Setting	Description
Check AUTN	<p>By default, this option is disabled.</p> <p>When the option is enabled, then UE will check the value of AUTN in the <i>Authentication Request</i> messages and it will reply with <i>Authentication Failure (MAC failure)</i> in case of different MAC values or with <i>Authentication Failure (Synch failure)</i> in the case the sequence number computed using the AUTN value is invalid.</p>
Unsolicited Router Advertisement	Select to enable this option.
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.
Identity Request PEI Type	<p>When the Identification Procedure is triggered by the MME/AMF due to the AMF Force Identification During Registration option being enabled, it allows the selection of the requested PEI type: IMEISV or IMEI.</p> <p>Default value: IMEISV.</p>
Always Include Uplink Data Status IE in Service Request Message	The UE will always include the Uplink Data Status IE for a Service Request message, not only if it has pending data.
Enable Passthrough	<p>Select this option to enable passthrough and any interface.</p> <p>Applicable to all passthrough topologies (UE/gNB or UPF).</p> <p>Applicable to either direction: GTPu to IP or/and IP to GTPu.</p>
Attach/Register with GUTI	When the Primary Objective type is Subscribers Per Second, enabling this option will trigger a Registration/Attach Request with the type of user identity set to temporary identity (GUTI). When option is not enabled, the type of user identity in the Registration/Attach Request will be permanent identity.
Authentication with GUTI	<p>This option is available only when <i>Attach/Register with GUTI</i> option is enabled.</p> <p>When enabled, this option triggers authentication in case of attach (4G) / register (5G) with GUTI.</p>
Force Emergency Registration	<p>When this option is enabled, the UE will perform an Emergency registration (instead of Initial Registration).</p> <p>Only the primary objective's DNNs are taken into account when deciding if the UE performs an emergency registration. When the <code>dnnIdsToActivate</code> is present but empty in the primary objective, the Emergency Registration will not be performed even if there is a Secondary Objective that uses an emergency DNN.</p>




Setting	Description
Identity Type for Emergency Registration	Select an option from the drop-down list. Available options: SUCI or IMEISV .
Support SMS	When this is selected, a flag will be added in the Registration message advertising UE support for SMS over NAS feature.
Delay Before Indirect Forwarding Cleanup (ms)	The time that will elapse before indirect forwarding cleanup. The delay is calculated from the UE Context Release.
Send Native GUTI During IRAT Mobility Registration	Enable this option to send native GUTI during IRAT mobility registration.
Authentication During Mobility Registration	Select a value from the drop-down list: <ul style="list-style-type: none"> • Never: Authentication is not performed during mobility registration. • Always: Authentication during mobility registration is always performed. • No Native Context: Authentication during mobility registration is performed only when the UE does not hold a native 5G security context.
Update GUTI in TAU	Select to enable this option.
<i>Radio Capability</i>	
UE Radio Capability IE Value for LTE	The UE radio capability IE value that will be included UE Capability Info Indication message.
UE Radio Capability IE Value for NR	The UE radio capability IE value that will be included UE Capability Info Indication message.
Send UE Capability IE Indication after Initial Context Setup	Enable this option to sent UE capability IE indication after initial context setup.
Trigger UE Radio Capability Check Procedure after Registration	This option will trigger from CoreSim the UE radio capability check procedure after registration in 5G or UE radio capability match procedure after attach in 4G.
Replay UE Radio Capability	<p>The UE Radio Capability IE is replayed in the Initial Context Setup Request and UE Radio Capability Match / Check messages on 4G and 5G. This option is applicable for the AMF and MME nodes.</p> <div> NOTE It is not applicable for Initial Context Setup Request of an inter-RAT handover procedure. </div>


Setting	Description
	<div>NOTE</div> <p>After UE Radio Capability Match / UE Radio Capability Check procedures, UE always sends UE Radio Capability Info Indication.</p>
<i>Location Reporting</i>	<i>Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).</i>
Reporting Type	<p>Select the value from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • Direct - If the test timeline is long enough, the AMF generates n LocationReportingControl messages at every m seconds from the moment Registration Complete message is received by the AMF (n is the value configured for Number of Repeats and m is the value of Interval Between Requests). • Change of Serving Cell - In case of Handover with AMF change, if Change of Serving Cell is selected, after handover, the new AMF will send a LocationReportingControl message to the NG-RAN.
Interval Between Requests (seconds)	Set the time interval between requests.
Number of Repeats	Set the number of repeats.
Start Time (seconds)	The number of seconds after successful attach when the AMF sends a LocationReportingControl message (event-type: change-of-serve-cell).
Stop Time (Seconds)	The number of seconds since the Start Time when the AMF sends LocationReportingControl message (event-type: stop-change-serving-cell).
<i>SMF Initiated PDU Session Release</i>	<i>Select the check box to enable this option.</i>
Time to Wait before SMF Initiated PDU Session Release (s)	Time in seconds to wait before SMF initiated PDU session release.
DNNs	<p>Select the DNNs from the drop-down list.</p> <p>The available options are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list.
<i>Network Initiated Deregistration</i>	<i>Select the check box to enable this option.</i>

Setting	Description
Time to wait before Network Initiated Deregistration (s)	Time in seconds to wait before network initiated deregistration.
Set Reregistration Required Flag in Deregistration Request Message	Enable this option to set a required reregistration flag in the deregistration request message.
AMF Initiated UE Context Release	Select the check box to enable this option.
Time to Wait before AMF Initiated UE Context Release (s)	Time in seconds to wait before AMF initiated UE context release.
Location Services	<p>Select the check box to enable Location Services (as described in TS23271/23273). The Location Services procedures over the LPPa /NRPPa interface are detailed in TS36455/38455.</p> <div> NOTE When Location Services is enabled, at least 1 profile must be configured (a maximum of 15 profiles allowed). </div>

Location Services

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

Setting	Description
<i>Location Services:</i>	
	Select the Add LCS Profile button to add a new profile.
	Select the Delete LCS Profile button to remove the profile from your test configuration.
Trigger	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> • None - no trigger (default option). • UE Available - UE exits Idle mode. • Change of Area - UE performs handover with TAC change.
<i>E-CID Measurements:</i>	
	<p>Select the Add E-CID Measurements button to add a new measurement.</p> <div> IMPORTANT A maximum of 15 E-CID Measurements can be configured across all LCS Profiles for an UE range. </div>

Setting	Description
	Select the Delete E-CID Measurements button to delete the measurement from your test configuration.
Report Characteristics	Select an option from the drop-down list: <ul style="list-style-type: none"> • On Demand - information is needed on demand in real time. • Periodic - periodic E-CID measurement reports.
Measurement Quantities	Select an option (or more) from the drop-down list. The available options are: Cell-ID (default option), Angle of Arrival , Timing Advance Type 1 , Timing Advance Type 2 , RSRP , RSRQ . <div> NOTE No support for Inter-RAT Measurement Quantities and WLAN Measurement Quantities. </div>
Delay (ms)	This option is available only when the <i>Trigger</i> is set to None . It represents the time trigger for E-CID measurement initiation.
Periodicity	This option is available only when the <i>Report Characteristics</i> is set to Periodic . It represents the periodicity of E-CID measurement reports. The available options are: 120 ms, 240 ms, 480 ms, 640 ms, 1024 ms, 2048 ms, 5120 ms, 10240 ms, 1 min, 6 min, 12 min, 30 min, 60 min .
Duration (ms)	This option is available only when the <i>Report Characteristics</i> is set to Periodic . It represent the timer to trigger E-CID measurement termination.

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

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

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

UE Subscribed AMBR settings



Each UE range has a set of **Subscribed AMBR** settings that configure the Aggregate Maximum Bit Rate (AMBR) for which the UEs in the range are subscribed.

Setting	Description
<i>Subscribed AMBR:</i>	
Subscribed AMBR Uplink	The subscribed uplink UE AMBR value for this range of UEs. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.
Subscribed AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Subscribed AMBR Downlink	The subscribed downlink UE AMBR value for this range of UEs. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.
Subscribed AMBR Downlink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.

DNNs Config

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

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

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

Setting	Description
SSC Mode	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) that had been allocated to the UE. SSC Mode 3: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Session ID	Provide the session ID value.
Deactivation Delay (s)	Delay measured from PDU Session Establishment until CN initiated selective deactivation of the User Plane connection.
Reactivation Delay (s)	Delay measured from CN initiated selective deactivation of a User Plane connection until UE initiated reactivation (Service Request in CM-Connected Mode).
DNN	Select one of the previously-defined DNNs from the drop-down list.
Local IPv4 Address	<p>The IPv4 address that the UE receives from the SMF during PDU Session Establishment. This address is used for L4-7 traffic (source IP for the UL traffic, destination IP for the DL traffic).</p> <p>IP address is also used to create UE Routes from DN.</p>
Local IPv4 Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Local IPv4 Address Increment	The value by which the IP addresses will be incremented.
Configure S-NSSAI:	<p><i>When this check-box is selected, you can configure which slice (S-NSSAI) to be send in PDU Session Establishment messages. If the check-box is not selected, the first slice from Allowed NSSAI list (received in Registration Accept) is used in PDU Session Establishment message.</i></p> <div> <p>NOTE</p> <p><i>This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</i></p> </div>
S-NSSAI	This list contains all the slices defined for the selected UE range. Select from the drop-down list the slice to be used in PDU Session Establishment.

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

SMS Configuration

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

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

Untrusted WiFi Settings

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

Setting	Description
Remote N3IWF	Select the remote N3IWF range from drop-down list.
Destination Port	Read-only field. Value set to 500 .
Source Port	Provide the source port. By default, set to 500 .

Setting	Description
NAS IP Type	Select the NAS IP type from the drop-down list: IPv4 (default) or IPv6 .
Configure a CA Certificate	By default this option is disabled. When enabled, the CA Certificate drop-down is displayed which allows the selection of one of the CA Certificates defined in global settings .
CA Certificate	Select the CA Certificate from the drop-down list.
<i>IKE Phase 1</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC , AES-192-CBC , AES-256-CBC , AES-128-GCM-16 , AES-192-GCM-16 , AES-256-GCM-16 .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: NONE . Available options: NONE , HMAC-MD5-96 , HMAC-SHA1-96 , HMAC-MD5-128 , HMAC-SHA1-160 , HMAC-SHA2-256-128 , HMAC-SHA2-384-192 , HMAC-SHA2-512-256 . Restrictions: <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. • If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	Select an option from the drop-down list. Default value: prime256v1(19) . Available options: prime256v1(19) , secp384r1(20) , secp521r1(21) , prime192v1(25) , secp224r1(26) , x25519(31) , x448(32) .
PRF Algorithm	Select an option from the drop-down list. Default value: HMAC-SHA256 . Available options: HMAC-MD5 , HMAC-SHA1 , HMAC-SHA256 , HMAC-SHA384 , HMAC-SHA512 .
<i>IKE Phase 2</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC , AES-192-CBC , AES-256-CBC , AES-128-GCM-16 , AES-192-GCM-16 , AES-256-GCM-16 .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: NONE . Available options: NONE , HMAC-MD5-96 , HMAC-SHA1-96 , HMAC-MD5-128 , HMAC-SHA1-160 , HMAC-SHA2-256-128 ,

Setting	Description
	HMAC-SHA2-384-192, HMAC-SHA2-512-256. Restrictions: <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	Select an option from the drop-down list. Default value: ID_DER_ASN1_DN . Available options: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER_ASN1_DN, ID_KEY_ID .
Local Identification Value	Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR .
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: 0 (disabled).

Network Slicing settings

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

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

The **Network Slicing** settings include:

UE NSSAI settings **76**

UDM SNSSAI Mappings 77

UE NSSAI settings



Each UE range requires at least one NSSAI range.

An NSSAI (Network Slice Selection Assistance Information) is a collection of S-NSSAIs (Single Network Slice Selection Assistance Information). An NSSAI may be a Configured NSSAI, a Requested NSSAI, or an Allowed NSSAI. A maximum of eight S-NSSAIs can be sent in signaling messages between the UE and the Network. The Requested NSSAI signaled by the UE to the network allows the network to select the Serving AMF, Network Slice(s), and Network Slice instance(s) for the UE.

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

The NSSAI slices are the ones supported by UE (DNN mapping is done from here also) that will be sent in NAS messages (for example Registration, PDU Session Establishment).

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



Setting	Description								
<i>UE NSSAI:</i>									
	Select the Add UE NSSAI button to add a new UE NSSAI to your test configuration.								
<i>UE NSSAI settings:</i>									
	Select the Delete UE NSSAI button to delete this UE NSSAI from your test configuration.								
SST	<p>The value that identifies the SST (Slice/Service Type) for this S-NSSAI. SST comprises octet 3 in the S-NSSAI information element. The standardized SST values are:</p> <table> <tr> <th>SST</th><th>Value</th></tr> <tr> <td>eMBB</td><td>1</td></tr> <tr> <td>URLCC</td><td>2</td></tr> <tr> <td>MIoT</td><td>3</td></tr> </table>	SST	Value	eMBB	1	URLCC	2	MIoT	3
SST	Value								
eMBB	1								
URLCC	2								
MIoT	3								
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.								
Mapped SST	The Mapped configured Slice/Service Type (SST) value for this S-NSSAI.								
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this S-NSSAI.								

UDM SNSSAI Mappings

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

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

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

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

Objectives

In a CoreSIM 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.

Test Objective categories:

Control Plane Objective	78
About primary objectives	78
Primary Control Plane Objective	80
Secondary Control Plane Objective	82
Handover	83
Paging	85

Enter/Exit Idle	86
Create/Delete QoS Flows	87
Create/Delete PDU Sessions	89
SMS	90
User Plane Objectives	91
Stateless UDP Traffic	92
Data Traffic	94
Voice Traffic	98
Video OTT Traffic	113
DNS Client Traffic	116
ICMP Client	119
Capture Replay	120
Synthetic	122
UDG	124
Predefined Applications Traffic	128
Applications	130
Application Advanced Settings	133
TCP Settings	135
TLS Settings	136
RTP Settings	138

Control Plane Objective

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

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

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

About primary objectives

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

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

Active Subscribers

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

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

<i>Ramp down time:</i>	20000 / 1000 = 20s for subscribers to deregister
<i>Rate in ramp down time:</i>	1000 deregistrations per second

Subscribers Per Second

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

Consider a test with 20000 subscribers, configured with: a Subscribers per Second primary objective with a rate of 1000/s and a hold time of 10s, a secondary objective with a rate of 2000/s, and a Sustain time configured for 30 seconds.

Such a test will give the following results.

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

Primary Control Plane Objective

Control Plane Objectives are structured as Primary and Secondary objectives. The focus of the primary objectives is on the establishment of subscriber PDU sessions.

The following table describes the **Primary** control plane objectives.

Parameter	Description
Objective Type	<p>Select the desired Primary Objective Type:</p> <ul style="list-style-type: none"> • Active Subscribers: The test attempts to activate and maintain the configured objective throughout the entire sustain time. Deactivation procedures will start only at the end of the sustain time. • Subscribers Per Second: The test attempts to activate a specified number of subscriber sessions per second, within the rate and time parameters that you configure. <p>The panel will display the settings for the selected Objective Type.</p>
<i>Active Subscribers:</i>	
Ramp-up Rate	The number of UE registrations that the test will establish per second. In the current release, each UE registration establishes exactly one PDU session.
Sustain Time (s)	The duration of time (in Seconds) that each subscriber session will be active.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p>
Number of Retries	<p>This value indicates how many times UE/NGRAN will retry the Register or PDU Session Establishment procedures if any message from these procedures encounters an error (timeout or an error is received).</p> <p>The available options are:</p> <ul style="list-style-type: none"> • -1 : infinite retries for entire sustain time. • 0 (default value) : the retry option is disabled. • 1 to 127: the number of retries per UE (Register + PDU Session procedure).
<i>Subscribers Per Second:</i>	

Parameter	Description
Hold Time (s)	The number of seconds that each subscriber session will remain active. This is, therefore, the amount of time that will elapse between the subscriber attach and the subscriber detach. At the end of the session hold time, the subscriber performs the detach procedure.
Rate	The number of subscriber sessions to activate per second.
Sustain Time (s)	The duration of time (in Seconds) that the specified session activation rate will be maintained.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p>

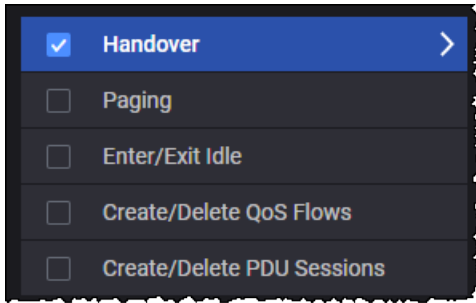
Secondary Control Plane Objective

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

IMPORTANT

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

In this example, only Handover has been selected:



Note that:

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

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

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

Handover



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

Handover configuration parameters

The following table describes these objective parameters.

Parameter	Description
<i>Handover:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which handovers are initiated, measured in procedures per second if

Parameter	Description
	Distributed over (s) is not modified.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Force N2 Handover	Enable this option to force N2 handover with direct forwarding instead of X2 / Xn handover.
Mobility for State	<p>This option specifies in what state should the UE perform the handover objective. The following options can be selected from the drop-down list:</p> <ul style="list-style-type: none"> • Connected • Idle • Any <p>When Any is selected, the UE will execute the handover objective, regardless if the UE is in Connected or Idle state.</p>
Force UE State Before Returning to Parent Node	<p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • None - The UE will perform either Idle Mode Mobility or Connected Handover to parent RAN, depending on what state the UE is before executing the procedure. • Connected - The UE will perform Connected Handover from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in idle state before performing this mobility, the UE will first perform exit idle, and only after the UE is in connected state, will it initiate the connected handover to the parent RAN. • Idle - The UE will perform Idle Mode Mobility from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in connected state before performing this mobility, the UE will first perform enter idle, and only after the UE is in idle state, will it initiate the idle mode mobility to the parent RAN.
Send Service Request after Returning to Parent Node	<p>By default, this option is disabled.</p> <p>Send Service Request immediately after Return to Parent Node Mobility if UE State was idle.</p>
Handover Cancel	<i>When this option is enabled, NG-RAN will trigger a Handover Cancel after receiving Handover Request from AMF. Handover Cancel is applicable only for N2</i>

Parameter	Description
	<i>Handover.</i>
Percentage	The percentage of N2 Handover Procedures that will trigger a Handover Cancel from the gNodeB.
Seed	The seed of Random Number Generator.
<i>Visited gNodeBs/eNodeBs/UNAPs : A list of the NG-RANs that UEs will visit during the test.</i>	
	Add next node to the list.
	Remove the selected node from the list.
Force UE State before Mobility	The following options can be selected from the drop-down list: <ul style="list-style-type: none"> • Connected • Idle • Any
Primary Node	Select the primary node from the drop-down list. If an UNAP is selected as the Primary Node, the Secondary Node field will not be displayed.
Secondary Node	Select the secondary node from the drop-down list.
Send Service Request After Mobility	By default, this option is disabled. Send Service Request immediately after Mobility if UE State was idle.

Paging

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

The following table describes the Paging objective parameters.

Parameter	Description
<i>Paging:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.

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

Notes:

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

Enter/Exit Idle

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

NOTE

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

The following table describes the objective parameters.

Parameter	Description
<i>Enter Exit Idle:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).

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

Create/Delete QoS Flows

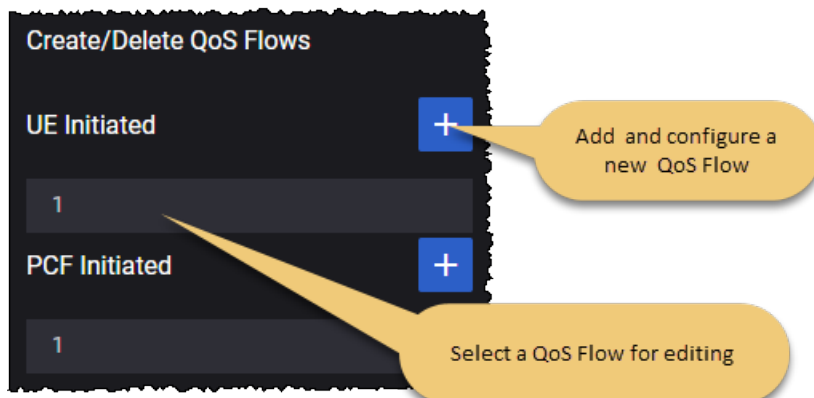
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured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

QoS flow options

There are two options for creating QoS flows:



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

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



Objective parameters

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

Parameter	Description
<i>Create/Delete QoS Flows:</i>	
	Select the Add Objective button to add an instance of this objective.
<i>Objective:</i>	
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this 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 for the drop-down list. For example: <code>dnn.keysight.com</code> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

Support for Network Initiated QoS Flow modification

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

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

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



Notes:

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

Create/Delete PDU Sessions

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

The following table describes the objective parameters.

Parameter	Description
<i>Create/Delete PDU Sessions:</i>	
	Select the Add Objective button to add an instance of this objective.
<i>Objective:</i>	
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	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	The maximum number of procedures that may be outstanding while new

Parameter	Description
Outstanding	procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	The interval between the triggering of creation and deletion of the PDU Session, in seconds.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p> <p>You configure DNNs for the selected UE in the DNNs Config Range settings. The list of available DNNs include those that have not been activated for the primary objective.</p>

SMS

This objective will perform the procedure of sending SMS messages.

The following table describes the objective parameters.

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

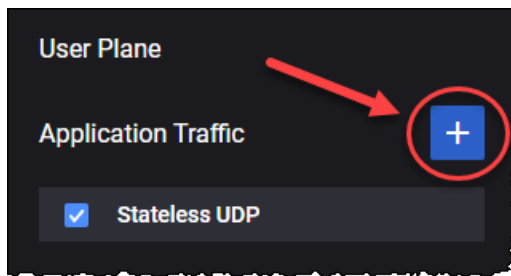
Parameter	Description
	start of sustain time.
Destination MSISDN	The MSISDN of the destination UE for the sent SMS.
Destination MSISDN Increment	The increment for the destination MSISDN.

NOTE No support for MT only SMS (CoreSIM initiated SMS).

User Plane Objectives


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


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



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

The following table describes the Application Traffic generation parameters.

Parameter	Description
	<p>Select this button to add a new application traffic objective. The objective can be:</p> <ul style="list-style-type: none"> • Stateless UDP • Data • Voice • Video OTT • DNS Client • Predefined Applications • ICMP Client • Capture Replay

Parameter	Description
	<ul style="list-style-type: none"> • 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 Ott Traffic .
DNS Client	For the settings required to configure the DNS Client objective, refer to DNS Client Traffic .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to Predefined Applications Traffic .
ICMP Client	For the settings required to configure the ICMP Client objective, refer to ICMP Client .
Capture Replay	For the settings required to configure the Capture Replay objective, refer to Capture Replay .
Synthetic	For the settings required to configure the Synthetic objective, refer to Synthetic .
UDG	For the settings required to configure the UDG objective, refer to UDG .

Stateless UDP Traffic

The **Stateless UDP** objective generates IP packets that encapsulate dummy UDP payload. The Stateless UDP generator configuration settings for the uplink traffic are described below.

The following table describes the Stateless UDP parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Flow Type	This field is set to uplink and can not be modified since on the UE you can only

Parameter	Description
	configure the uplink flow.
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.
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
Destination IP Address	The destination IP address to place in the IP packet.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>

Data Traffic


The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by CoreSIM 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 .
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	Set 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 UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .

Parameter	Description
Application Traffic Flows	<p>Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.</p> <ul style="list-style-type: none">• To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.• To add another traffic flow, click the Add Flow button. CoreSIM will open the Flow panel where you will select the flow type and configure the flow settings. <p>Refer to Flow for a description of the configuration settings for these traffic flows.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

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	<p>Select the transport protocol from the drop-down list. Available options:</p> <ul style="list-style-type: none"> If Optimize Throughput (per UE) option is enabled: TCP, TLS, QUIC or UDP. If Optimize Throughput (per UE) option is disabled: TCP, TLS or UDP.
Type	<p>Select the L4/L7 protocol type from the list of pre-defined flows. The available options are:</p> <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get, HTTP Put, HTTP Post and FTP. For TLS transport protocol: HTTPS Get, HTTPS Put and HTTPS Post. For QUIC transport protocol: HTTP3 Get, HTTP3 Put and HTTP3 Post. For UDP transport protocol: UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket) <div> <div>NOTE</div> <p>UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receives the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds.</p> </div>
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.
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.

Parameter	Description
URL	The URL that is being accessed by the flow's protocol.
Destination Hostname	Destination hostname of the server. If DNS hostname resolution is enabled for the flow and Name Servers are configured under Global Settings, this name will be resolved before being used as L7 destination IP for the flow and included in HTTP headers. If empty, the "Address" from the previous fly-out level will be used as L7 destination IP for the flow.
Max Transactions per Connection	Set the value for this parameter.
Enable DNS Query Per Connection	Select the check-box to process only one DNS query per TCP connection.
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range settings (DNNs Config).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

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

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

You can add custom parameters as follows:

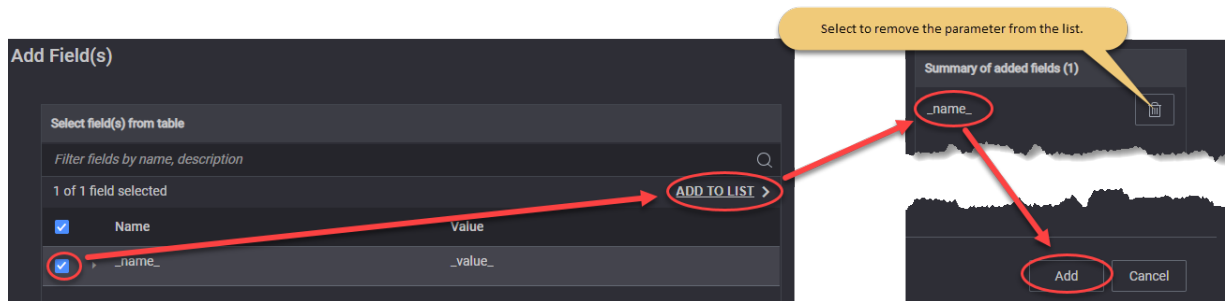
1. Select the **Open Custom Parameters** button.



The Custom Parameters panel opens.

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

For example ...



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

Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Call Type	<p>Select the type of call from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> • Basic Call • Basic Call Mo (Mobile Originated) • Basic Call Mt (Mobile Terminated)
Dial Plan:	For the settings required to configure the dial plan, refer to Dial Plan .
Sip Settings:	

Parameter	Description
Local Port	Set the local port number. You can accept the value provided by CoreSIM or overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security • UDP - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	For more details about these settings, refer to Advanced SIP Settings .
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by CoreSIM or overwrite it with your own value.
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select this option in order to enable RTCP.
<i>Audio settings:</i>	<i>For the configuration of audio settings, refer to Audio Settings.</i>
<i>Video Settings:</i>	<i>For the configuration of video settings, refer to Video Settings.</i>
<i>MSRP Settings:</i>	<i>For the configuration of MSRP settings, refer to MSRP Settings.</i>
<i>Advanced Media Settings:</i>	
<i>Custom SDP</i>	<i>Select this panel to open the custom SDP settings.</i>
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4

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



Dial Plan

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

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

Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for audio from the drop-down list.
<i>Jitter Buffer Settings:</i>	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
<i>Audio Codecs</i>	
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	<p>Select the audio codec from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • AMR - The Adaptive Multi-Rate (AMR) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • AMR-WB - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • EVS - The EVS (Enhanced Voice Services) codec specified by 3GPP TS 26.445 compresses 20ms input blocks of audio samples. In addition to the EVS Primary mode, 3GPP TS 26.445 specifies that the codec implement the EVS AMR-WB IO mode for interoperability with AMR WB devices. • PCMU • PCMA • iLBC • G722 • G723 • G729 <p>The parameters of each audio codec are presented below.</p>

AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.

Parameter	Description
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> • Bandwidth efficient: In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added. • Octet aligned: In the octet-aligned format, all the fields in a payload, including payload header, table of contents entries, and speech frames themselves, are individually aligned to octet boundaries to make implementations efficient. All fields of an AMR payload (payload header, table of contents and speech) are individually octet aligned.
Bitrate	<p>Indicates the mode(bitrate) of the AMR codec.</p> <p>For AMR there are 8 available modes. All these modes can be changed dynamically without negotiation, reflecting the main characteristics of this codec – adaptive rate.</p> <p>For AMR WB there are 9 modes available.</p>

EVS



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

PCMU/PCMA/iLBC/G722/G723/G729

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

Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Voice	Select the QoS Flows ID(s) from the drop-down list.
<i>Video Codecs</i>	<i>This section is available only when Enable video is selected</i>
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: H264 or H265 .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

MSRP Settings

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

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

Advanced SIP Settings

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

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

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

SIP Custom Headers

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

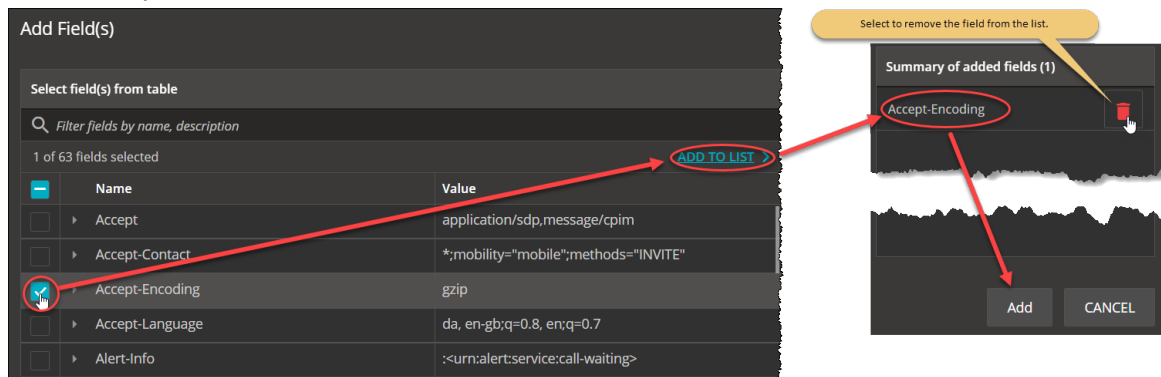
NOTE

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

For each message, you can:

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

For example ...



The following custom header are available:

Parameter	Description	Value
Accept	IETF RFC 3261	application/sdp,message/cpim
Accept-Contact	IETF RFC 3841	*;mobility="mobile";methods="INVITE"
Accept-Encoding	IETF RFC 3261	gzip
Accept-Language	IETF	da, en-gb;q=0.8, en;q=0.7

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

Parameter	Description	Value
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC 3261	3600
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC	60

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

Parameter	Description	Value
Preferred-Service	RFC 6050	
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

Parameter	Description	Value
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
Subscription-State	IETF RFC 6665	active

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

SIP Authentication

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

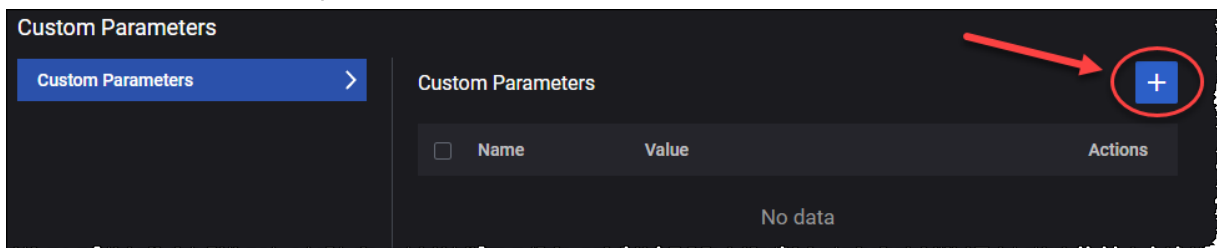
Parameter	Description
Username	Provide the username.
Password	Provide the password.
Authentication Type	Select the authentication type: <ul style="list-style-type: none"> • Digest MD5 • AKAv1 • AKAv2 • ProxyDefined
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by CoreSIM, 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	Select the operator-specific authentication value.

Parameter	Description
OPc	
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 CoreSIM, 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 CoreSIM, or enter of an OP value of your own choosing.
Opc Increment	The number used to increment the OPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same OPc value.

Custom Parameters

You can add custom parameters as follows:

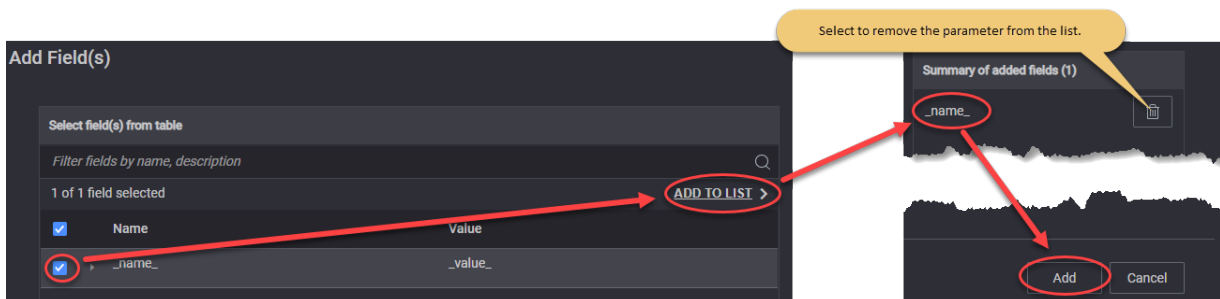
1. The Custom Parameters panel, select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom parameters are available:

Parameter	Description	Value
DelayBefore SIPInvite	Delay in milliseconds before sending SIP INVITE.	1000

Parameter	Description	Value
DealyBeforeRTP	Delay in milliseconds before RTP session start.	0
DelayAfterRTP	Delay in milliseconds 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 milliseconds before 180 Ringing message will be sent.	0
DelayBefore200INVITE	Delay in milliseconds before 200 OK message for INVITE will be sent.	0
debugIPSEC	Activate IPSEC debug. Please use debug only for a reduced number of simulated UEs.	0
timeoutSIP	Global timeout in milliseconds for any SIP message. Default is set to standard 32000ms. Use this parameter to modify the default value.	32000
MaxActiveLimit	Set maximum allowed concurrent TCP connections per CPU Core. Default it is set to 8000. Please use this parameter to modify the default value.	8000

SIP 3GPP IPSEC

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

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

Video OTT Traffic


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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Objective Type	Select the value from the drop-down list: Simulated Users or Throughput .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example,for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
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 .
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. <ul style="list-style-type: none"> To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings. To add another traffic flow, click the Add Flow button. CoreSIM will open the Flow panel where you will select the flow type and configure the flow settings.
Flow:	

Parameter	Description
	Select this button to remove this flow from your test configuration.
Type	Select the Ott traffic type from the drop-down list. Available options: <ul style="list-style-type: none"> • DASH • HLS
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
URL	Select the URL from the drop-down list populated with the defined on the server.
Play Until End	If this check box is selected, the Play Duration field is disabled and the original playtime is used.
Play Duration (sec)	This field is available only if the Play Until End check box is not selected. It allows you to set a custom playtime.
Transport	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/QUIC
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero).
Percentage	The percentage of Test Objective to execute this flow.
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
<i>Jitter Buffer:</i>	
Initial Delay (s)	Set the number of seconds to wait before playback. The default value is 20.
Maximum Size (s)	Set the number of seconds to be buffered on the client side.

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

Advanced Client Settings

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

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

Custom Parameters and Headers

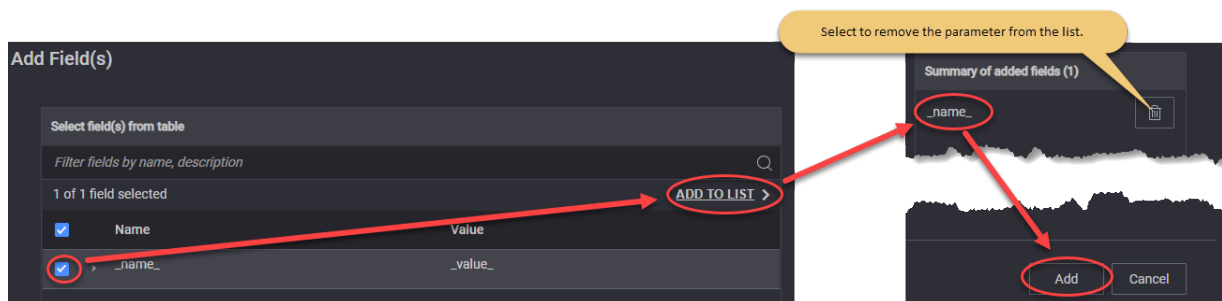
From this section you can add custom parameters or custom header fields:

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

You can add custom parameters as follows:

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

For example ...



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

DNS Client Traffic


The following table describes the DNS Client Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to DNS Client .

Parameter	Description
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Connection multiplier (per UE)	Set the value for the connection multiplier.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Application Traffic Flows	<p>Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"> • To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings. • To add another traffic flow, click the Add Flow button. CoreSIM will open the Flow panel where you will select the flow type and configure the flow settings. <p>Refer to Flow for a description of the configuration settings for these traffic flows. Also, you can add custom parameters, based on your test configuration requirements.</p>

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Type	By default, the type is set to DNS Client .
Port	The port used by the flow.
DNS Server IP	Set the DNS server IP address.
Number of DNS servers	Set the number of DNS servers.
Hostname	Set the hostname.
Query Type	Select the query type from the drop-down list. The available options are: <ul style="list-style-type: none"> • 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.
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Config).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

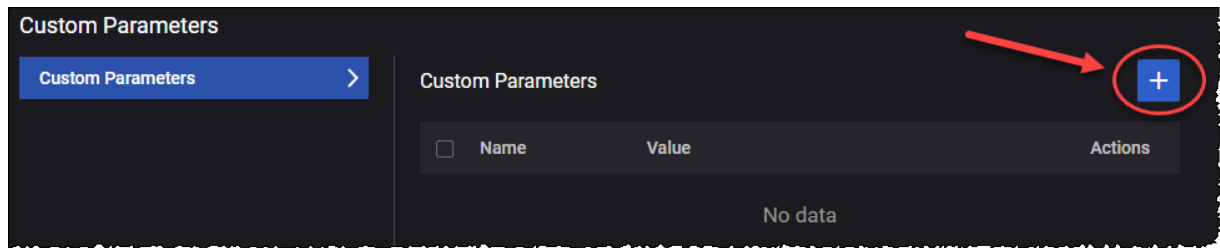
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

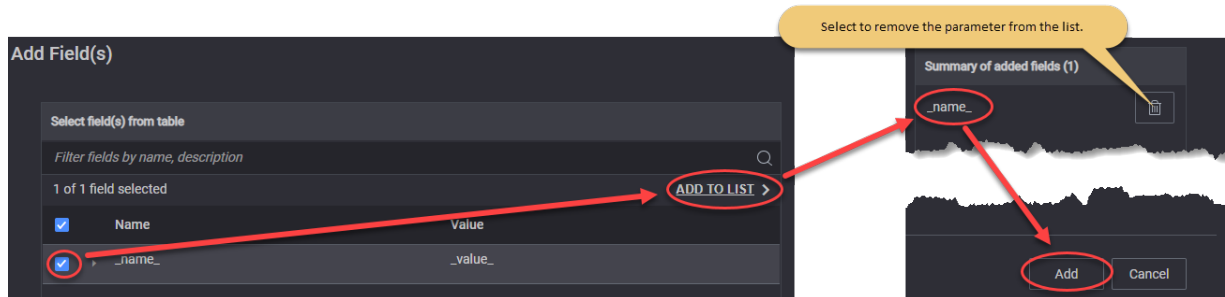
2. Select the **Add** button.



The Add Field(s) opens.

- 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 value provided by CoreSIM or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Traffic Flow	Refer to Traffic Flow for a description of the configuration settings for these traffic flows.

Traffic Flow

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

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

Capture Replay



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

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Capture Replay .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Capture File	It allows you to upload a capture file, using the Upload button. To remove the file, select the Clear button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to 0 for no limit. The default value is 1 .
Maximum Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Rx Timeout (ms)	Time the responder waits for packets, after the delay observed in the packet capture. The default value is 1000 milliseconds.
Delayed Tx	Prevent the packets from being sent faster than they appear to be sent in the

Parameter	Description
	capture file, trying to maintain the packet delays. The default value is true (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is true (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.

The following table describes the Filter object parameters.

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

Parameter	Description
	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 <code>pcap-filter</code> format, as described at https://www.tcpdump.org/manpages/pcap-filter.7.html .
Remove Encapsulation	Remove GTPu encapsulation from packets, if present, before trying to match the filter expression and when replaying the packets. The default value is false (option disabled).
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to Initiator . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Synthetic .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.

Parameter	Description
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the UDP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the UDP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).

Parameter	Description
Max source port	The Max value specifies the upper bound (the highest permissible port number).

The following table describes the Traffic Flow parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
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 UDG parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to UDG .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	If necessary, enable this option.

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

The following table describes the Traffic Flow parameters.

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

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

The following table describes the UDG Traffic Parameters.

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

Parameter	Description
<i>Ping-pong</i>	
Ping Direction	Set the ping direction. Available options: Upstream or Downstream .
Ping Interval	Set the ping time interval.
Ping Interval Unit	Set the ping interval unit. Available options: Millisecond or Microsecond .
Pong Number	Set the value for the pong number.
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.

The following table describes the Transaction parameters.

Parameter	Description
<i>Transaction</i>	<i>Select the check-box to enable these settings.</i>
Duration (ms)	Transactions duration, in millisecond.
Idle interval (ms)	Idle interval between transactions, in millisecond.
Resume Mode	Side which triggers transition between the UE idle and the UE connected state. Available options: User or Network .

Predefined Applications Traffic

The following table describes the Predefined Flows Traffic parameters.

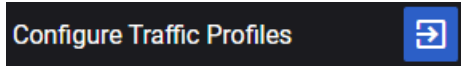
Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Simulated Users • Throughput • Connections Per Second
Throughput (kbps)	<div>IMPORTANT</div> This parameter is available only when Objective Type is set to Throughput . The desired throughput (in kbps) for the combined traffic flows that will be generated.

Parameter	Description
Connections Per Seconds	<div> <div>IMPORTANT</div> <div>This parameter is available only when Objective Type is set to Connections Per Second.</div> </div> <p>Set the number of connections.</p>
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	<p>The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.</p>
Configure Traffic Profiles	<p>Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions.</p> <p>Refer to Traffic Profile for a description of the configuration settings for these traffic profiles.</p>

Traffic Profile

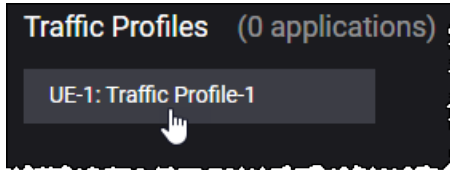
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



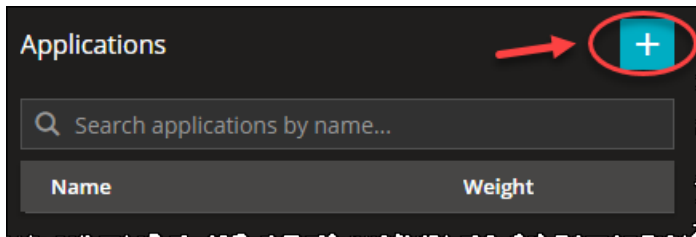
The Traffic Profile Configuration section opens.

3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:
 - [Applications](#)
 - [TCP Settings](#)
 - [TLS Settings](#)
 - [RTP Settings](#)

Applications

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

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



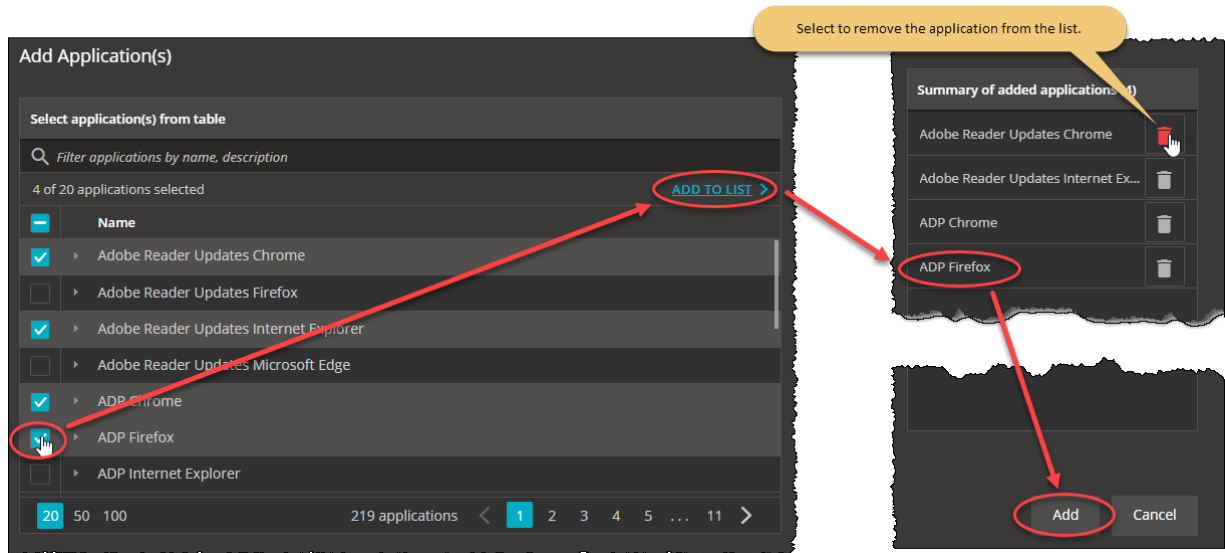
The Add Application(s) window opens.

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

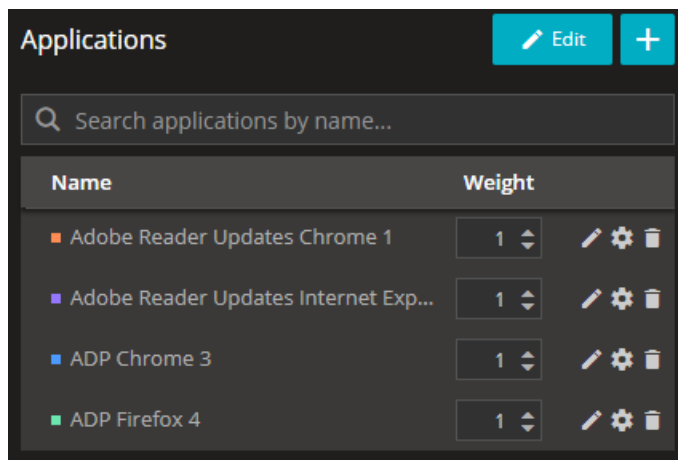
NOTE

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

For example ...




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



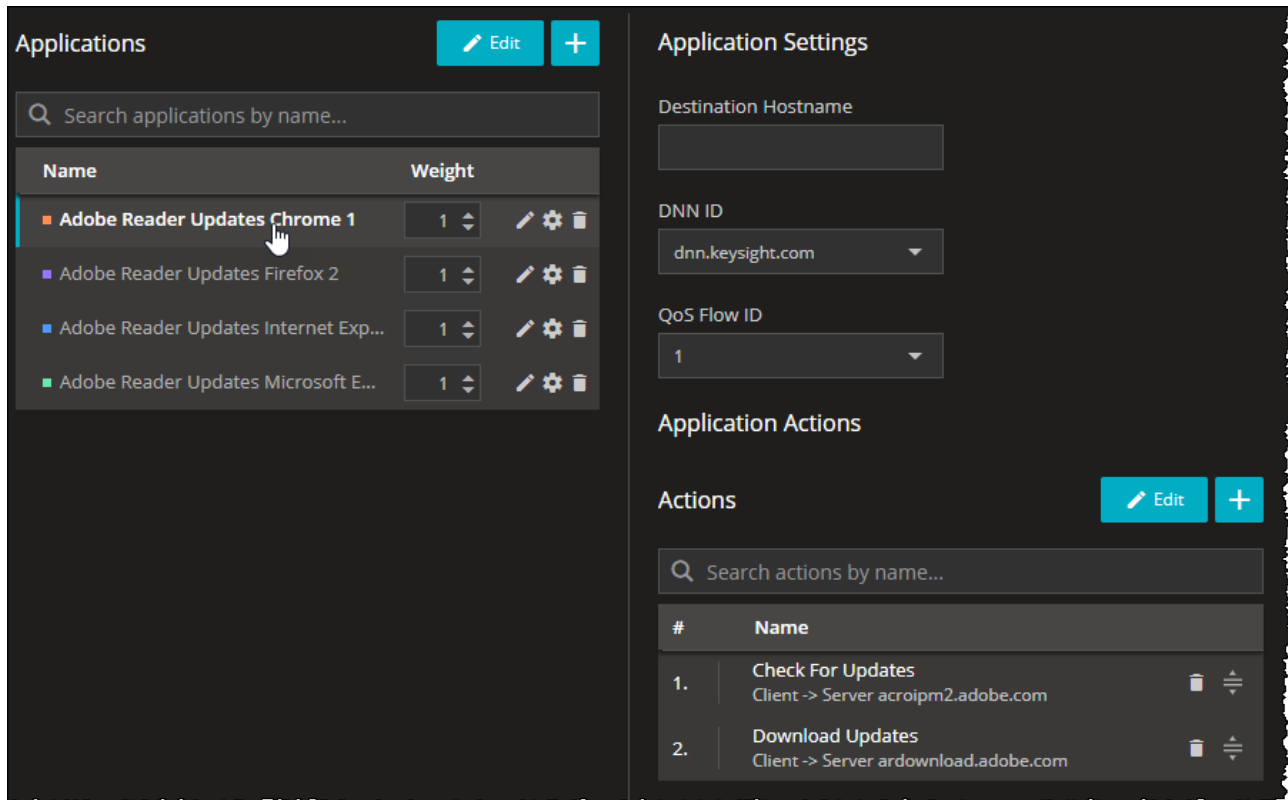
3. If needed, you can select the **Edit** button to enable the bulk selection of the available applications in order to remove them from the list.

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

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

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

For example ...



Application Settings

Under the Application Settings section, the following fields are displayed:

NOTE

These fields under the Application Settings section are common to all predefined applications.

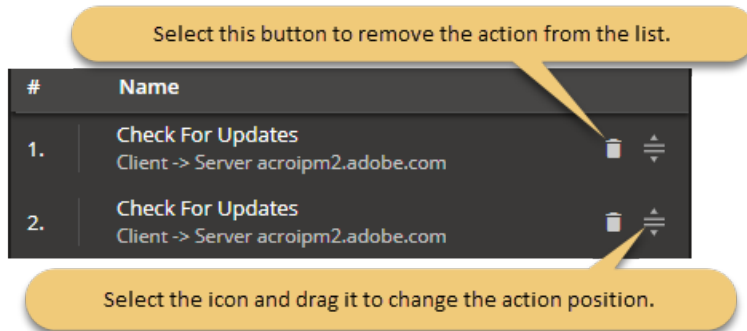
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

Application Actions

The Application Actions section lists the actions and action parameters available in CoreSIM for each predefined application. For the complete list of actions and parameters, refer to [Application Actions](#).

Under the Application Actions section, you can edit or add new actions for each application:

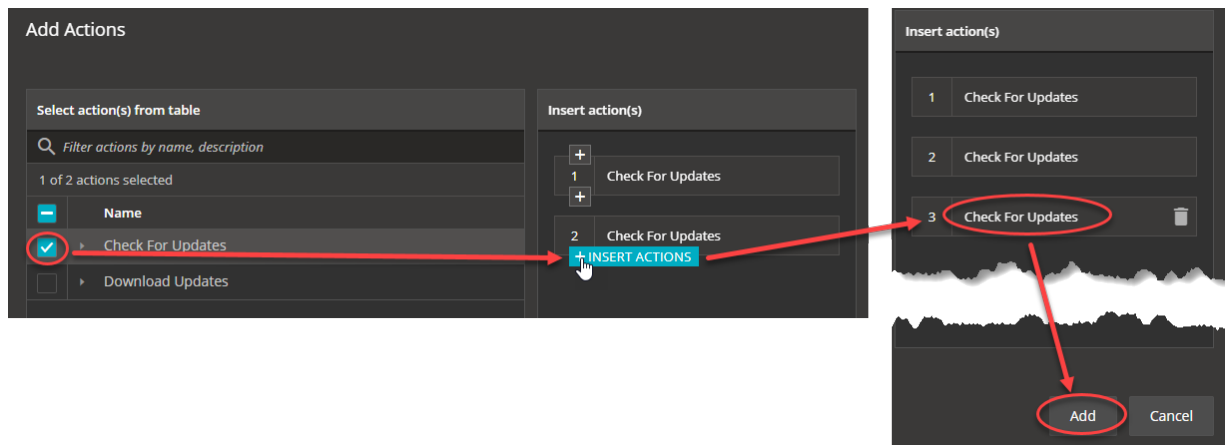
1. Use the icons available for each icon in order to remove it or to change its position in actions list.
For example ...



2. Select the **Add Actions** button to add new actions to the application. The Add Action(s) window opens.

Select an action from the list and then use the **Insert Actions** button to add the action in the desired position on the Insert Action(s) table. Select **Add**.

For example ...



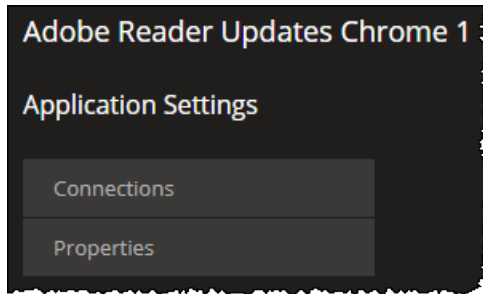
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

Application Advanced Settings

For each predefined application, the Application Settings menu is displayed when the Advanced Settings button is selected. This menu contains two main sections:

- **Connections**
- **Properties**

For example ...



Under the **Connections** section, the Connections table is displayed. When a connection is selected, the Connections Properties fields are displayed, as follows:

Field	Description
Name	The application name.
Client Endpoint	The client endpoint.
Server Endpoint	The server endpoint.
Hostname	The hostname name.
Destination Port	The TCP source port that the client endpoint is initiating connections from.
Server Port	The TCP port that the server endpoint is accepting connections on.
Encryption disabled	Select the check box to enable it this option.

Under the **Properties** section, the application settings Properties fields are displayed, as follows:

Field	Description
Name	The application name.
Iterations	Set the value for the number of iterations.
Max Transactions	The maximum amount of transactions an application can make.
Client HTTP profile	Select the client HTTP profile from the drop-down list. The available options are: <ul style="list-style-type: none"> • Chrome • Firefox • Opera • Microsoft Edge • Internet Explorer • Safari • Android
Action Timeout	Set the action timeout in seconds.

Field	Description
(seconds)	
Connection Persistence	<p>Select an option for the connection persistence:</p> <ul style="list-style-type: none"> • Standard - inherits the behavior with respect to the HTTP version (1.0 or 1.1). • Disabled - enforces connection closing following every HTTP message. • Enabled - enforces connection persistence through explicit keep-alive.
HTTP Version	<p>Select the HTTP version used:</p> <ul style="list-style-type: none"> • HTTP/1.0 • HTTP/1.1

TCP Settings

These parameters are configurable for both Client and Server settings, as presented in the following table.

Parameter	Description
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number). The default value is 1024.
Max source port	The Max value specifies the upper bound (the highest permissible port number). The default value is 65535.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test

Parameter	Description
	network, increase the size of the transmit buffer to improve the throughput.
Enable RFC1323 TCP timestamps	<p>Enable or disable the stamp using the toggle button. If enabled, the client or server inserts an RFC 1323 timestamp into each packet.</p> <p>NOTE Enabling the TCP Timestamp option adds 12 bytes to the TCP header. This reduces the effective configured MSS.</p>

TLS Settings

NOTE

TLS multi version support is available, you can configure both TLS 1.2 and TLS 1.3 from **Client TLS Settings**. You can choose multiple ciphers for each different version. The Client sends these versions and ciphers in the Client Hello and the Server chooses one of the versions and ciphers and replies back with Server Hello. The Client then proceeds with the handshake.

NOTE

Once you select either of the two Session Reuse Methods below for the **Client TLS Settings**, you can specify how many simultaneous connections can share the same Session ID or Ticket through the **Session Reuse Count** option for **TLSv1.2**.

These parameters are configurable for both Client and Server settings, as presented in the following tables.

Client TLS Settings

Parameter	Description
<i>TLSv1.2</i>	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <p>NOTE Session reuse method is available only if TLSv1.2 is selected.</p>
Immediate close	Select the check box to enable it.
<i>TLSv1.3</i>	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatilby	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.

Parameter	Description
Immediate close	Select the check box to enable it.

Server TLS Settings

Parameter	Description
<i>TLSv1.2</i>	<i>Select the check box to enable it.</i> <i>The following options became available:</i>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	Select the Session Reuse Method from the drop-down list: <ul style="list-style-type: none"> • Disable • Session ticket • Session ID <div>NOTE</div> Session reuse method is available only if TLSv1.2 is selected.
Immediate close	Select the check box to enable it.
<i>TLSv1.3</i>	<i>Select the check box to enable it.</i> <i>The following options became available:</i>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibilty	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	Select the check box to enable it.
<i>SNI Enabled</i>	<i>Select the check box to enable the server name indicator. The following SNI Settings become available:</i>
Certificate file	Select Upload to add your certificate file or Clear to remove it.
Key file	Select Upload to add your key file or Clear to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select Upload to add your DH file or Clear to remove it.
<i>Certificate file</i>	<i>Select Upload to add your certificate file or Clear to remove it.</i>
<i>Key file</i>	<i>Select Upload to add your key file or Clear to remove it.</i>

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

RTP Settings

The following elements are available on the RTP Settings tab under the Traffic Profile Configuration section.

Settings	Description
Encryption Mode	Select an encryption mode from the drop-down list. Available options: None , XOR , ZOOM or SRTP .
MOS Mode	Select the Session Reuse Method from the drop-down list. Available options: Disable , Per interval or Per call .

DN configuration settings



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

The configuration settings are described in the topics listed below.

Topics:

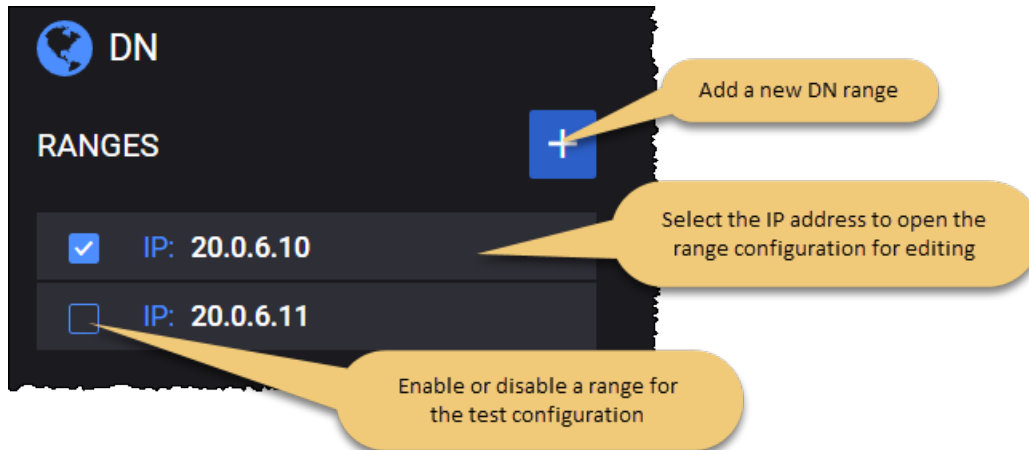
DN Ranges panel	139
DN Range panel	139
DN N6 interface settings	140
DN routes settings	141
DN User Plane	142
DN Stateless UDP Traffic	143
DN Data Traffic	144
DN Voice Traffic	147
DN Video OTT Traffic	158
DN DNS Server Traffic	161
DN Predefined Applications Traffic	163
DN Capture Replay	164
DN Synthetic	166
DN UDG	168

DN Ranges panel

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

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

For example ...



DN Range panel


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

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

DN range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.

Setting	Description
Range Count	The number of DNs in the DN range.
<i>Range Settings:</i>	
N6 Interface Settings	Each DN range requires the configuration of N6 interface settings, through which a DN instance enables connectivity and interaction with other functions in the 5G network. These settings are described in DN N6 interface settings .
Routes Settings	These settings are described in DN routes settings .
User Plane	These settings are described in DN User Plane .

DN N6 interface settings

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



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

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>

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

DN routes settings

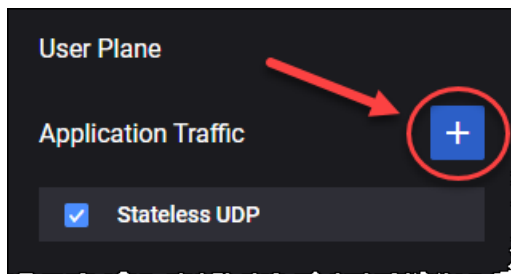
The following table describes the **Route Settings** that you need to configure in order to create the route to an UE or custom range.

Settings	Description
<i>Routes Config:</i>	
	Select this button to add a new route to a specific UE range or a custom one.
<i>UE Routes Config:</i>	
	Select this button to remove the route.
Route Type	Select the route type from the drop-down list. Available options: UE or Custom .
UE Range MSIN	Select the MSIN of the UE range from the drop-down list.
Peer UPF	Select the UPF node connected to DN over the N6 interface from the drop-down list.
Gateway Address	The IP address assigned as gateway address.
DNN(s)	Select the DNNs from the drop-down list. The available options are: <ul style="list-style-type: none"> All: Select this item to choose all of the available DNNs that are configured for the UE. specific DNNs: Select one or more of the individual DNNs from the list.
Destination	Set the destination subnet address.

Settings	Description
Subnet Address	This parameter is available only when the route type is set to Custom .
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. This parameter is available only when the route type is set to Custom .



DN User Plane

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



NOTE

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

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

Parameter	Description
Voice	For the settings required to configure the Voice traffic objective, refer to DN Voice Traffic .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to DN Video OTT Traffic .
DNS Server	For the settings required to configure the DNS Server objective, refer to DN DNS Client Traffic .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to DN Predefined Applications Traffic .
Synthetic	For the settings required to configure the Synthetic objective, refer to DN Synthetic .
UDG	For the settings required to configure the UDG objective, refer to DN UDG .

DN 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 value provided by CoreSIM or overwrite it with your own value.
Flow Type	This field is set to downlink and can not be modified since on the DN you can only configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
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	The source port number to place in the UDP header.

Parameter	Description
Port	
Destination UE Range	Select the destination UE range from the drop-down list.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>

DN 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 value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Application Servers	<p>Each Application Traffic entry requires an application server definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"> To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.

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

Server

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

Parameter	Description
	Click the Delete Server button to remove the application server from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: TCP, TLS, QUIC or UDP .
Type	Select the L4/L7 protocol type from the list of pre-defined application servers. The available types include: <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get Responder, HTTP Put Responder, HTTP Post Responder, HTTP Server and FTP Responder. For TLS transport protocol: HTTPS Get Responder, HTTPS Put Responder, HTTPS Post Responder and HTTPS Server. For QUIC transport protocol: HTTP3 Server. For UDP transport protocol: UDP Bidirectional Responder.
Port	The port used by the application server.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.
QoS FlowID	Select a QoS Flow ID for this application server.
Client Tx Count	This parameter is available only when the application server type is set to UDP Bidirectional.
Server Tx Count	This parameter is available only when the application server type is set to UDP Bidirectional.

Custom Parameters

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

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

You can add custom parameters as follows:

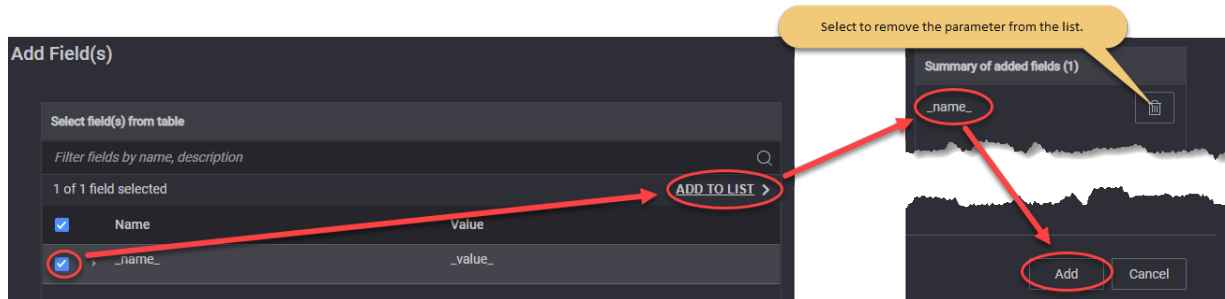
1. Select the **Open Custom Parameters** button.



The Custom Parameters panel opens.

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

For example ...



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

DN Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
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 CoreSIM or overwrite it with your own value.
Transport Protocol	<p>Select the transport protocol. The available options are:</p> <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security

Parameter	Description
	<ul style="list-style-type: none"> • 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 .
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by CoreSIM 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.
<i>Audio settings:</i>	<i>For the configuration of audio settings, refer to Audio Settings.</i>
<i>Video Settings:</i>	<i>For the configuration of video settings, refer to Video Settings.</i>
<i>MSRP Settings:</i>	<i>For the configuration of MSRP settings, refer to MSRP Settings.</i>
<i>Advanced Media Settings:</i>	
<i>Custom SDP</i>	<i>Select this panel to open the custom SDP settings.</i>
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4 • NB Codecs IPv6 • AMR-WB IPv6 • Multimedia IPv4
<i>QoE Settings</i>	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).



Dial Plan

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

Parameter	Description
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.

Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for audio from the drop-down list.
<i>Jitter Buffer Settings:</i>	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
<i>Audio Codecs</i>	
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	<p>Select the audio codec from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • AMR - The Adaptive Multi-Rate (AMR) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • AMR-WB - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • EVS - The EVS (Enhanced Voice Services) codec specified by 3GPP TS 26.445 compresses 20ms input blocks of audio samples. In addition to the EVS Primary mode, 3GPP TS 26.445 specifies that the codec implement the EVS AMR-WB IO mode for interoperability with AMR WB devices. • PCMU • PCMA • iLBC

Parameter	Description
	<ul style="list-style-type: none"> • G722 • G723 • G729 <p>The parameters of each audio codec are presented below.</p>

AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> • Bandwidth efficient: In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added. • Octet aligned: In the octet-aligned format, all the fields in a payload, including payload header, table of contents entries, and speech frames themselves, are individually aligned to octet boundaries to make implementations efficient. All fields of an AMR payload (payload header, table of contents and speech) are individually octet aligned.
Bitrate	<p>Indicates the mode(bitrate) of the AMR codec.</p> <p>For AMR there are 8 available modes. All these modes can be changed dynamically without negotiation, reflecting the main characteristics of this codec – adaptive rate.</p> <p>For AMR WB there are 9 modes available.</p>

EVS

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



Parameter	Description
	the EVS codec bitrates for the EVS Primary or EVS AMR-WB IO mode.
Bitrate	Indicates the mode(bitrate) of the EVS codec. Select the value from the drop-down list.

PCMU/PCMA/iLBC/G722/G723/G729

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

Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Voice	Select the QoS Flows ID(s) from the drop-down list.
Video Codecs	<i>This section is available only when Enable video is selected</i>
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: H264 or H265 .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

MSRP Settings

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

Parameter	Description
Enable MSRP	Select to enable this option.

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

Advanced SIP Settings

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

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

SIP Custom Headers

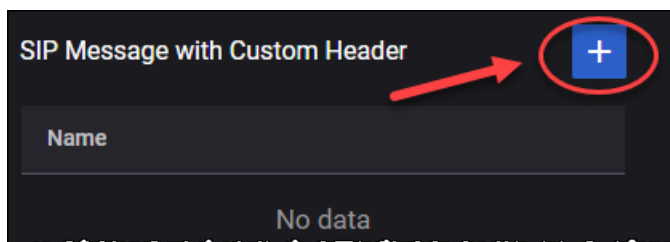
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE

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

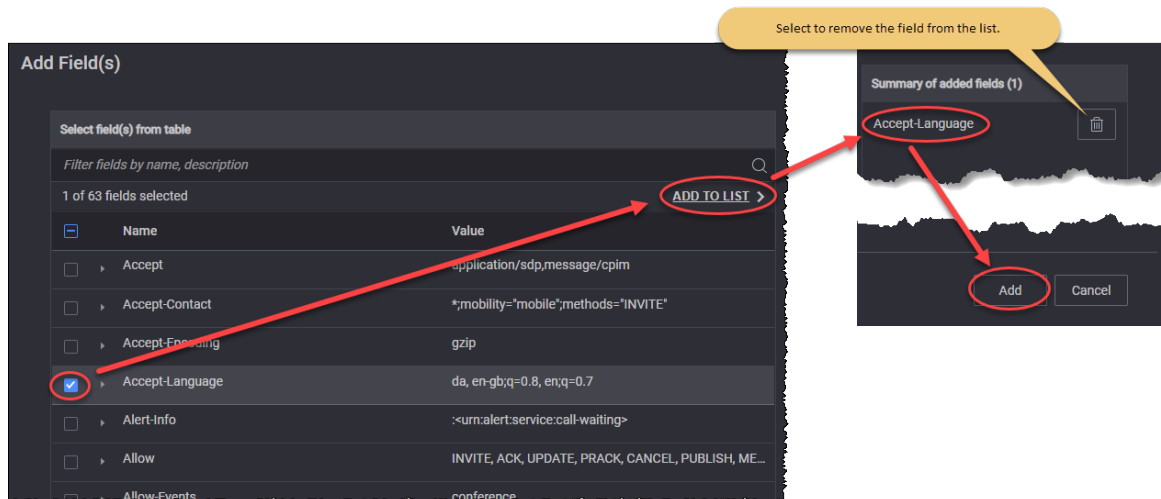
For each message, you can:

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



The Add Field(s) opens.

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



The following custom header are available:

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

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

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

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

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

SIP Authentication

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



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

Parameter	Description
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by CoreSIM, 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 CoreSIM, 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 CoreSIM, or enter of an OP value of your own choosing.
OPc Increment	The number used to increment the OPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same OPc value.

DN Video OTT Traffic

The following table describes the Video OTT Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example,for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
<i>OTT Servers:</i>	



Parameter	Description
	Select this button to add an OTT server to your test configuration.
	Select this button to remove the OTT server from the test configuration.
Server Name	Set the server name. Each server is identified by a unique name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Transport	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/QUIC
Port	Set the port number. You can accept the value provided by CoreSIM 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.



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

Parameter	Description
	Select this button to add a stream to your test configuration.
	Select this button to remove the stream from the test configuration.
Stream Name	Set the stream name. Each server is identified by a unique name. You can accept the value provided by CoreSIM or overwrite it with your own value.
URL	Set the URL path.
Type	Select the stream type from the drop-down list: <ul style="list-style-type: none"> • Real • Synthetic

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

Custom Parameters

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

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

You can add custom parameters as follows:

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

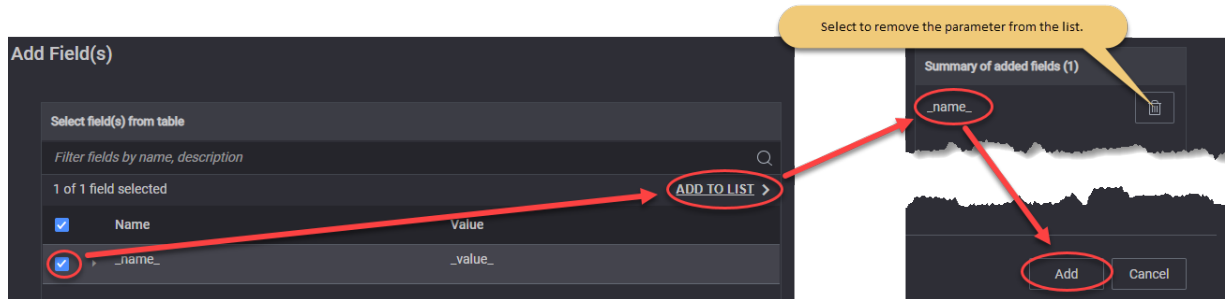


The Custom Parameters panel opens.

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

- 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.

DN DNS Server Traffic

The following table describes the DNS Server Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to DNS Server .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
<i>DNS Servers:</i>	
	Select this button to add an DNS server to your test configuration.
	Select this button to remove the DNS server from the test configuration.
Type	Select the type from the available options.
Port	Set the port number. You can accept the value provided by CoreSIM or overwrite it with your own value.





Parameter	Description
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.



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

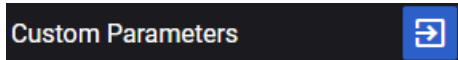
Parameter	Description
	Select this button to add a zone to your test configuration.
	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by CoreSIM or overwrite it with your own value.
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: <ul style="list-style-type: none"> • A • AAAA • CNAME • TXT • PTR • NS

Parameter	Description
Hostname	Set the hostname.
Adress	Provide the address.

Custom Parameters

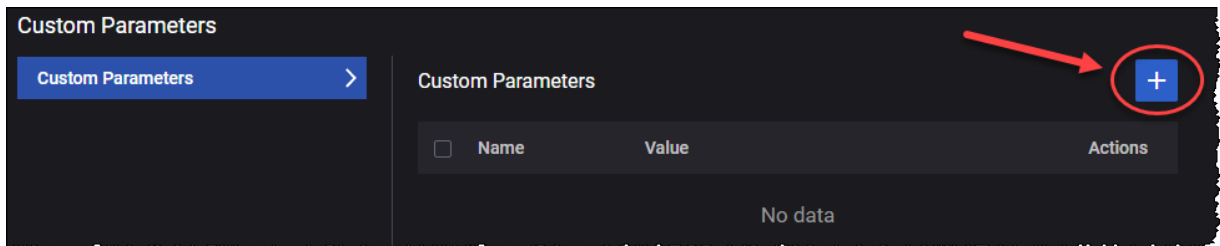
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

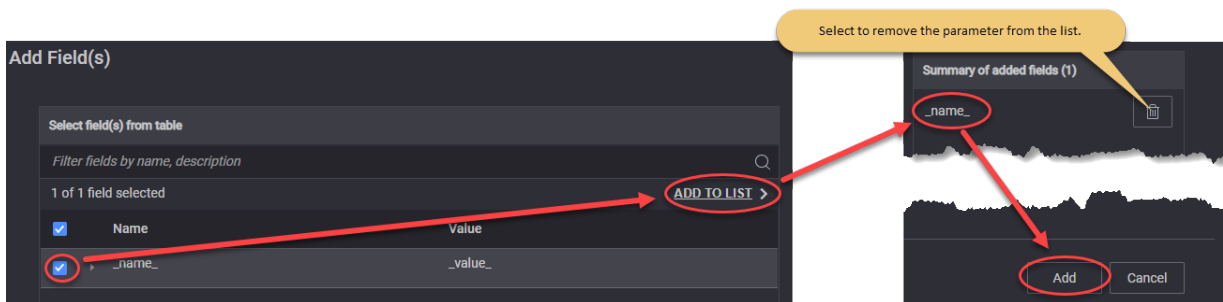
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DN Predefined Applications Traffic

The following table describes the Predefined Applications parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be

Parameter	Description
	generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Predefined Traffic Profiles	Select the traffic profile from the available options.



DN Capture Replay

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Capture Replay .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Capture File	It allows you to upload a capture file, using the Upload button. To remove the file, select the Clear button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to 0 for no limit. The default value is 1 .
Maximum Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Rx Timeout (ms)	Time the responder waits for packets, after the delay observed in the packet capture. The default value is 1000 milliseconds.
Delayed Tx	Prevent the packets from being sent faster than they appear to be sent in the capture file, trying to maintain the packet delays. The default value is true (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is true (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .

Parameter	Description
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.

The following table describes the Filter object parameters.

Parameter	Description
<i>Filter</i>	
	Select this button to add a new filter to your test configuration.
	Select this button to remove the additional route from your test configuration.
Role	<p>Select the role from the drop-down list. Available options: Initiator and Responder.</p> <p>Default value: Initiator.</p>
Filter Expression	<p>This field cannot be empty. It selects the packets to be replayed from uploaded capture. The filter string should be in <code>pcap-filter</code> format, as described at https://www.tcpdump.org/manpages/pcap-filter.7.html.</p>
Remove Encapsulation	<p>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).</p>

Parameter	Description
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to Initiator . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

DN Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Synthetic .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then

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

The following table describes the Traffic Flow parameters.

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

Parameter	Description
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

DN UDG

The following table describes the UDG parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to UDG .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).

Parameter	Description
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the UDP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the UDP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).

The following table describes the Traffic Flow parameters.

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

The following table describes the Out of Band Signaling parameters.

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

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

IMS configuration settings

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

In CoreSIM, IMS has two important components:

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

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

Topics:

CSCF Range panel	170
Media Function Range panel	171

CSCF Range panel

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

CSCF range controls and settings

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

Setting	Description
<i>P-CSCF Node Settings</i>	
Domain	Set the domain name.
Port	Set the port number. You can accept the value provided by CoreSIM or overwrite it with your own value.
<i>Authentication</i>	

Setting	Description
<i>Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: keysight.com .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: Digest , AKAv2 or AKAv1 .
Algorithm	Select the algorithm from the drop-down list. Available options: MD5 , MD5-Sess , SHA256 or SHA256-Sess .
Quality of Protection	Select an option from the drop-down list: auth or auth-init .
<i>Connectivity Settings</i>	
IP Address	Set the IP address.

Media Function Range panel

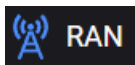
When you select the Media Function's IP address from the **Media Function Ranges** panel, CoreSIM opens the **Range** panel, from which you can configure the connectivity settings for the Media Function range.

Media Function range controls and settings

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

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

RAN/Untrusted AP configuration settings



In wireless networks, a Radio Access Network (RAN) is the network that enables user endpoints, such as mobile phones, to communicate and access core network resources.

The test topology supports both the 5G gNodeB and the 4G eNodeB. In each case, the RAN provides access and coordinates the management of resources across the radio sites. Multiple instances of RAN may be deployed. In 5G topology, an *untrusted AP* refers to an Access Point that is considered unsecure or not fully trusted by the cellular network operator.

The configuration settings are described in the topics listed below.

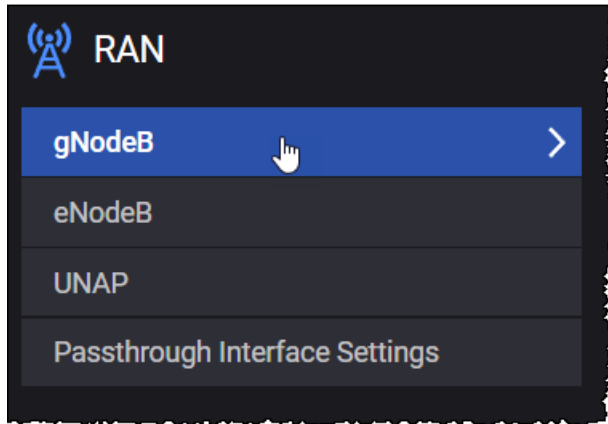
Topics:

gNodeB **172**

gNodeB Ranges panel	173
gNodeB Range settings	176
gNodeB node settings	177
gNodeB NSSAI settings	180
gNodeB N2 interface settings	181
gNodeB N3 interface settings	185
eNodeB	189
eNodeB Ranges panel	189
eNodeB Range Settings	193
eNodeB Node Settings	194
S1-U Interface Settings	195
S1-MME Interface Settings	196
UNAP	198
UNAP Ranges panel	198
UNAP Range Settings	199
Passthrough interface settings	200

gNodeB

To configure one or more gNodeB ranges for a test, select gNodeB from the RAN panel.



The following topics describe the gNodeB configuration settings:

gNodeB Ranges panel	173
gNodeB Range settings	176
gNodeB node settings	177
gNodeB NSSAI settings	180

gNodeB N2 interface settings	181
gNodeB N3 interface settings	185

gNodeB Ranges panel

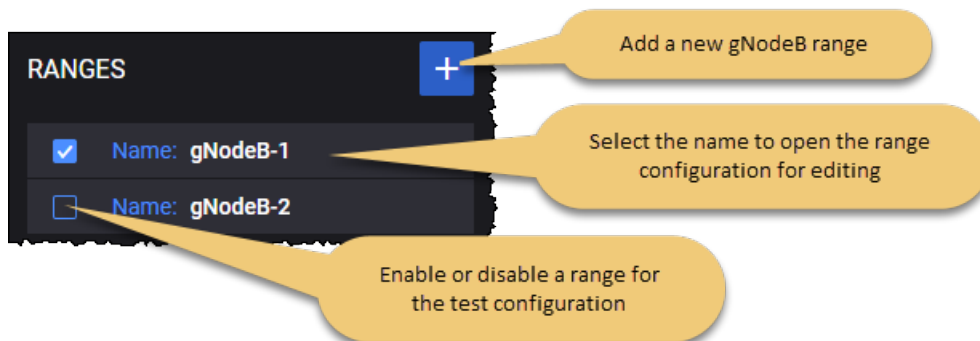
The **gNodeB Ranges** panel opens when you select **gNodeB** from the RAN pane. It consists of two main sections: Ranges and Ranges Connectivity.

Ranges

On the Ranges section, you can perform the following task:

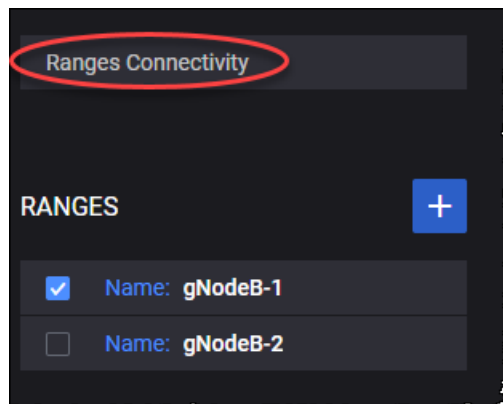
- Add a new gNodeB range to your test configuration.
- Open a gNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



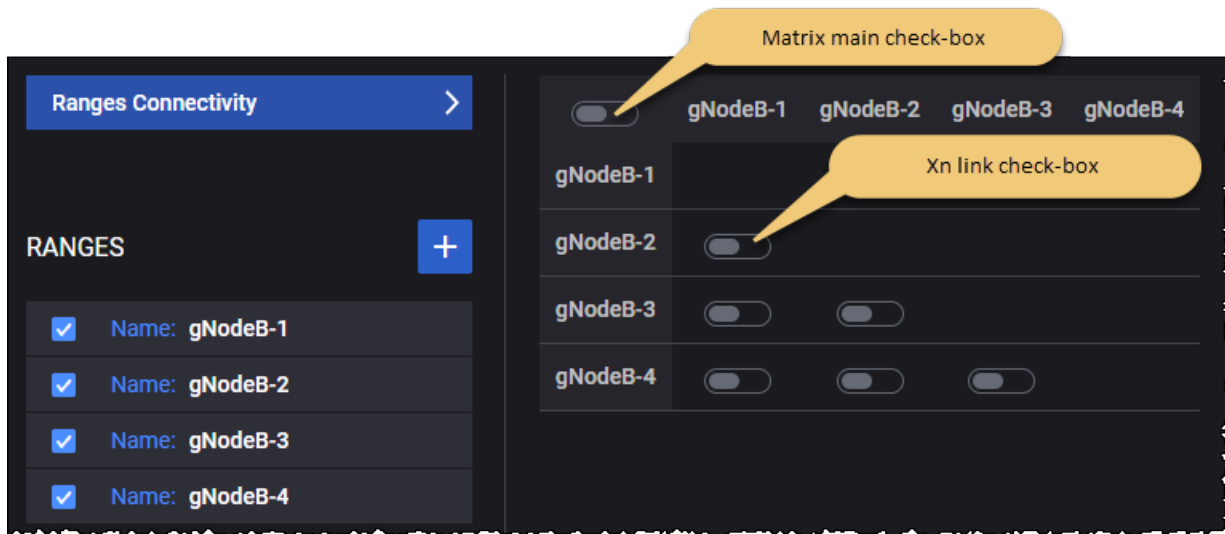
Ranges Connectivity

The Ranges Connectivity section allows you to configure Xn links between gNodeB ranges for handovers. This section is displayed as a matrix of check-boxes, each selected check-box represents an Xn link between ranges on the line and the range on the column.



Note that to configure the Xn links between gNodeB ranges, you need to add at least two gNodeB ranges. If there are fewer than two gNodeB ranges, CoreSIM displays the following message: "Two or more ranges are required to configure Xn links".

Due to the fact that the Xn links are bidirectional the Range Connectivity matrix is only half full of check-boxes.



Each Xn link check-box can have one of the following states:

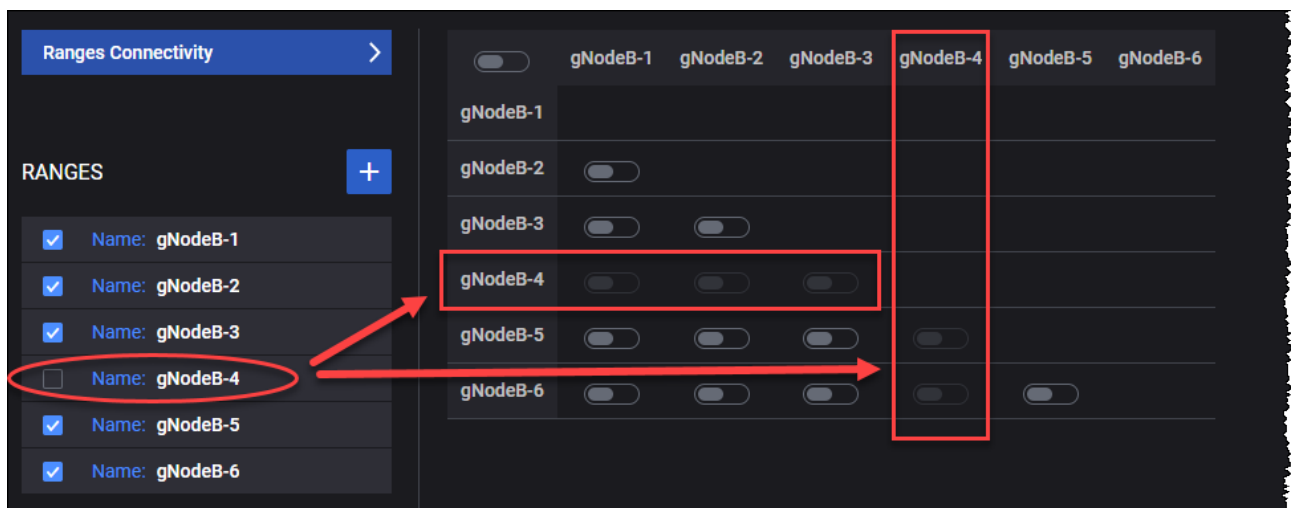
State	Description
Selected and blue color	An Xn link connection is established between enabled gNodeB ranges.
Selected and grey color	An Xn link connection is established between disabled gNodeB ranges.
Unselected	No Xn link connection between gNodeB ranges.

To see all the Xn links for a particular gNodeB range, you need to read the line of that range and then the column of that range.

If none of the links is marked as an Xn link then only N2 handovers will be performed.

Hovering over a specific gNodeB range from the Ranges Connectivity matrix highlights the row and displays more details about the connectivity/range status.

When a gNodeB range is disabled you are not able to select any Xn link for that specific gNodeB range.



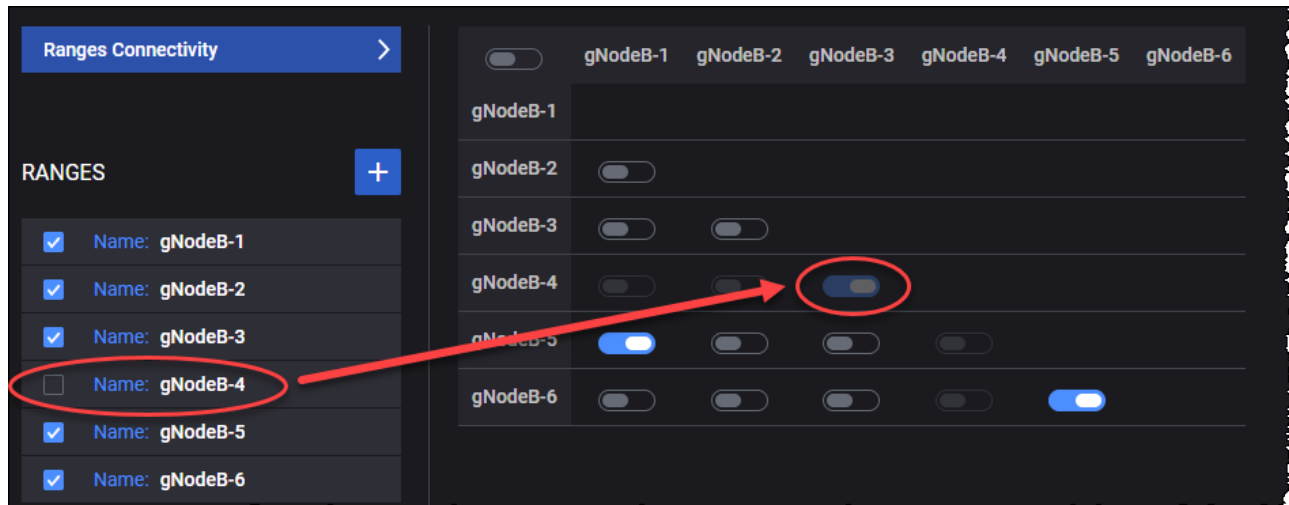
If there was an Xn link between two gNodeB ranges and now one of them is disabled, the check-box will become greyed out and cannot be unselected.

NOTE

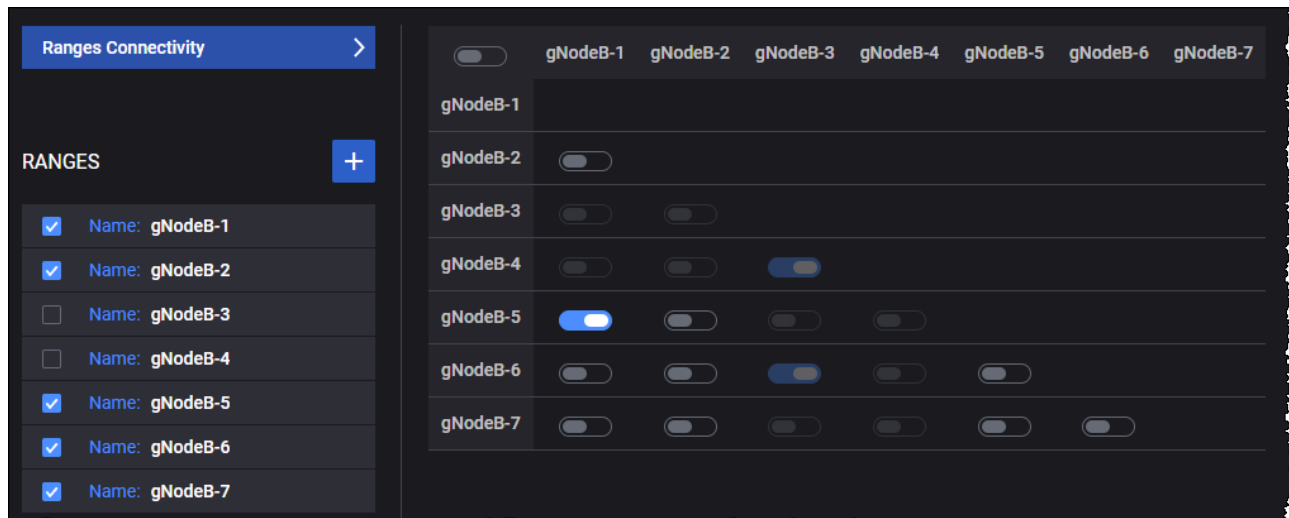
None of the Xn links that are part of disabled gNodeB ranges are sent to the traffic agent.

For example ...

1. The disabled range gNodeB-4 had an Xn link with gNodeB-3. The selected check-box is greyed out. This Xn link will not be sent to the traffic agent.



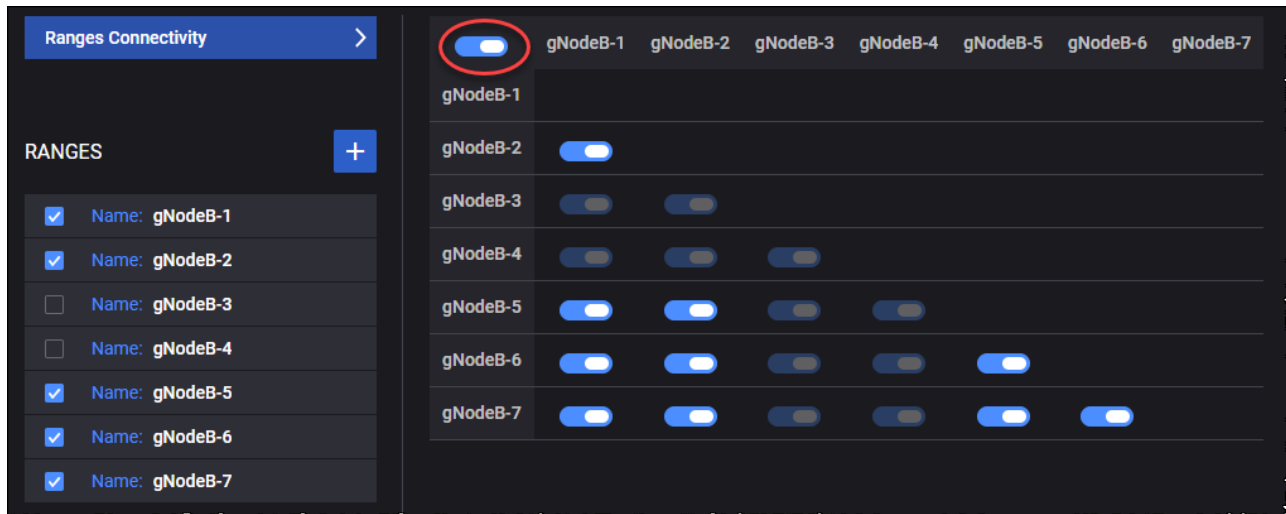
2. The gNodeB-3 range was enabled on previous step and there were selected Xn links between gNodeB-3/gNodeB-4 and gNodeB-3/gNodeB-6. Due to the fact that gNodeB-3 is now disabled, the check-box for Xn links between gNodeB-3 and gNodeB-6 have become greyed out.



The first cell of matrix contains a main check-box that displays the state of the matrix and perform operations.

State	Description	Operation
Selected	All connected.	If the main check-box is Selected, you can undo the selection to change the state to Unselected and all Xn links from the connectivity matrix will become unselected (none connected).
Unselected	None connected.	If the main check-box is Unselected, you can select it to change the state to Checked and all Xn links from the connectivity matrix will become selected (all connected).

When the main matrix check-box is selected all the Xn link check-boxes from the matrix become selected.



Even the Xn link check-boxes for disabled gNodeB ranges are selected since the Xn links for disabled gNodeB ranges are not sent to the traffic agent. This way, when the disabled gNodeB range is enabled, you will not have to manually select the Xn link check-boxes for that particular gNodeB range.

gNodeB Range settings


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

- Delete the gNodeB range from the test configuration.
- Designate the range as a **Device Under Test**.
- Specify the number of gNodeB nodes to configure for the range.
- Select **Range Settings** to configure the node and connectivity settings for the gNodeB range.

gNodeB range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Device Under Test	Enable this option if your gNodeB is a DUT in this test configuration. When this option is not enabled, the CoreSIM will simulate the gNodeB functionality (if it is selected in the Topology window).
Range Count	The number of gNodeBs in the gNodeB range.
<i>Range Settings:</i>	
Node Settings	Each gNodeB range requires the configuration of an associated set of Node Settings, which are describe in gNodeB node settings .
NSSAI	Each gNodeB range requires the configuration of at least one NSSAI, and may specify multiple NSSAIs. These settings are described in gNodeB NSSAI settings .
N2 Interface Settings	Each gNodeB range requires the configuration of N2 interface settings, through which a gNodeB instance enables connectivity and interaction with the AMF component in the 5G network. These settings are described in gNodeB N2 interface settings .
N3 Interface Settings	Each gNodeB range requires the configuration of N3 interface settings, through which a gNodeB instance enables connectivity and interaction with the UPF component in the 5G network. These settings are described in gNodeB N3 interface settings .

gNodeB node settings

Each gNodeB range includes a set of Node Settings.

Node Settings

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

Setting	Description
Name	Multiple gNodeB instances may be deployed in the 5G network. Each gNodeB instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by CoreSIM or overwrite it with your own value.
PLMN MCC	The PLMN MCC for this gNodeB range.
PLMN MNC	The PLMN MNC for this gNodeB range.
Tracking area	The Tracking Area Code to use for the nodes in this range.

Setting	Description
code	
gNodeB ID	The gNodeB Identifier. It is used to uniquely identify each gNodeB within a PLMN. The gNodeB ID is contained within the NCI of its cells. When the gNodeB <i>Range Count</i> setting is greater than 1, CoreSIM increments the <i>gNodeB ID</i> setting for each gNodeB.
gNodeB ID Length	The number of bits from the Cell Identity to use as the gNodeB ID.
Cell ID	The NR Cell Identity (NCI) for the cell associated with this node range.
Connection Timeout (ms)	The S1AP connection timeout.
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.

EPS Fallback Settings

The **Enable EPS Fallback** check box enables the UE to switch from the 5G core network (5GC) to a LTE/EPS connection in order to avoid bad connection quality. This is done using a 5G to 4G inter-RAT handover (during which the session management and user plane tunnels in the core network are handed over from SMF/UPF to MME/S-GW).

The following parameters are required to configure the EPS fallback:

Setting	Description
Enable EPS Fallback	Select the check box to enable this option.
5QI	Select the 5G QoS identifier that will trigger the EPS fallback procedure. (The 5QI must be defined on the QoS Flow configuration settings panel in the Global Settings .) When a request is received for this 5QI to create a dedicated QoS flow, the RAN will reject the request, which will trigger the EPS fallback procedure.
Associated ENB	Select the eNodeB used for handover.
Secondary Node	Select the secondary node from the drop-down list. This option is used for EPS fallback to an eNodeB associated to a gNodeB using Option 3x.
EPS Fallback Mobility	Type of mobility to EPS during EPS fallback. Select an option from the drop down list: <ul style="list-style-type: none"> • Handover to 4G

Setting	Description
	<ul style="list-style-type: none"> • Inter-System Redirection to 4G
EPS Fallback Return Mobility	<p>Type of mobility that occurs after the deletion of the dedicated bearer that triggered EPS fallback.</p> <p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • None - After the dedicated bearer is deleted in 4G, the UE will not initiate any procedure. • Connected Mode Handover to 5G (default value) - After the dedicated bearer is deleted in 4G, the UE will initiate a 4G to 5G Connected Mode Handover. • Idle Mode Mobility to 5G - After the dedicated bearer is deleted in 4G, the UE will perform an Enter Idle procedure in 4G, followed by a 4G to 5G iRAT Idle Mode Mobility.
Send Service Request After EPS Fallback Return Mobility	<p>By default, this option is disabled.</p> <p>Send Service Request immediately after returning to 5G when Idle Mode Mobility to 5G was performed.</p>

The following options can be enabled under the **User Plane Security** pane:

- Enable Integrity (by default, this option is disabled)
- Enable Confidentiality (by default, this option is disabled)

NOTE

User Plane Security settings are not taken into account for N2 Handover procedure.

The following parameters are required under the **Public Warning System** pane:

Setting	Description
<i>Public Warning System</i>	<i>Select the check box to enable this option.</i>
PWS Restart Timer (s)	<p>Duration in seconds after which PWS Restart Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38413</i> , <i>8.9.3 PWS Restart Indication</i>.</p> <p>Values should be in range 0-86400. Default value: 0.</p>
PWS Failure Timer (s)	<p>Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38413</i> , <i>8.9.4 PWS Failure Indication</i>.</p> <p>Values should be in range 0-86400. Default value: 0.</p>

NOTE

If the *Public Warning System* option is enabled and both PWS Restart and PWS Failure procedures are configured to be initiated (non-zero timers), the timers should be different.

gNodeB NSSAI settings

Each UE range requires at least one NSSAI range.

NSSAI (Network Slice Selection Assistance Information) includes one or more NSAIIs. Each network slice is uniquely identified by a specific NSSAI.

The slice assistance information comprises a list of one or more NSAIIs, where an NSSAI is a combination of:



- An 8-bit mandatory SST (Slice/Service Type) field, which identifies the slice type.
- An SD (Slice Differentiator) field, which differentiates among Slices that have the same SST field and consist of 24 bits.

An NSSAI information element identifies a network slice. In addition to the SST and SD, it can also include an optional Mapped Configured SST and an optional Mapped Configured SD.

For each gNodeB range in your test configuration, you can add and delete NSAIIs (NSSAI 1, NSSAI 2,...NSSAI X) as required to meet your test objectives.

The gNodeB NSSAI slices are the ones supported per TA level, that will be sent in NGAP messages (for example NG Setup).

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

Setting	Description												
NSSAI:													
	Select the Add NSSAI button to add a new NSSAI to your test configuration.												
NSSAI settings:													
	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 NSSAI information element. The standardized SST values are:												
	<table><tr><th>SST</th><th>Value</th><th>Suitable for handling:</th></tr><tr><td>eMBB</td><td>1</td><td>5G enhanced Mobile Broadband</td></tr><tr><td>URLCC</td><td>2</td><td>ultra-reliable low-latency communications</td></tr><tr><td>MIoT</td><td>3</td><td>massive IoT</td></tr></table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
	SST	Value	Suitable for handling:										
	eMBB	1	5G enhanced Mobile Broadband										
	URLCC	2	ultra-reliable low-latency communications										
MIoT	3	massive IoT											
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field												

Setting	Description
	comprises octets 4 through 6 in the NSSAI.
Mapped SST	The Mapped configure Slice/Service Type (SST) value for this specific NSSAI.
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this specific NSSAI.

gNodeB N2 interface settings

N2 is the user plane interface between the gNodeB and the AMF.

When the gNodeB node is used as secondary node on a UE Range (either in the Parent RAN > [Secondary Node](#) section or in the [Handover](#) objective), the option to enable/disable the N2 interface is displayed.

By default, the N2 interface check box is enabled.

When the gNodeB node is used only as secondary node on a UE Range ((either in the Parent RAN > [Secondary Node](#) section or in the [Handover](#) objective), the option to enable/disable the N2 interface is displayed.

The following configuration settings are required by each gNodeB N2 range.

N2 Interface Settings

Settings	Description
Peer AMF	The IP address of the AMF node connected to gNodeB over the N2 interface.
Destination port	The destination Stream Control Transmission Protocol (SCTP) port for control plane messages (NG-AP signaling messages) on the N2 interface.
SCTP source port	The source SCTP port for control plane messages (NG-AP signaling messages). Each SCTP endpoint provides the other endpoint with a list of transport addresses through which that endpoint can be reached and from which it will originate SCTP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP port. The default port number is 36412, but you can change it.
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum	Set the maximum retransmission timeout value, in milliseconds.

Settings	Description
Retransmission Timeout (ms)	
Initial Retransmission Timeout (ms)	Set the initial retransmission timeout value, in milliseconds.
Maximum Retransmission per Association	Set the maximum retransmissions value per association.
Maximum Retransmission per Path	Set the maximum retransmissions value per path.
Heartbeat Interval (ms)	Set the heartbeat interval value, in milliseconds.
SACK Delay (ms)	Set the delayed selective ACK timeout value.
SACK Frequency	Set the delayed selective ACK frequency value.

Connectivity Settings

Settings	Description
<i>IPSec: Select the check box to enable IPsec option.</i>	
Peer SEG	Select the peer SEG range from the drop-down list.
Destination Port	By default, the destination port is set to 500 and cannot be changed.
Source Port	Set the source port number.
Inner IP Type	Select the IP type: IPv4 or IPv6 .
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to Certificates and cannot be changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	It allows you to upload an archive that contains the certificates and keys for the gNodeB range, using the Upload button. To remove the archive, select the Clear button. The <code>.key</code> and <code>.crt</code> files need to have the same name before extensions.
Use Same Certificates and	By default, this option is disabled. Select the toggle button to enable it.

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

Settings	Description
	<p>is NONE.</p> <ul style="list-style-type: none"> If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list.</p> <p>Default value: ID_DER_ASN1_DN. Available options: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER_ASN1_DN, ID_KEY_ID.</p>
Local Identification Value	<p>Set the value for this parameter.</p> <p>This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR.</p>
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
DPD Interval (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Emulated Router Address	<p>Set the IPv4 or IPv6 address for the emulated router. This allows to hide all messages from the interface behind a MAC address.</p> <p>NOTE This option can be used only with IxStack stack.</p>
Emulated Router	Set the IP network mask for the emulated router.

Settings	Description
Address Prefix Length	
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<div>IMPORTANT</div> <i>This option is visible only when the Outer VLAN check-box is selected.</i> <i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID..

gNodeB N3 interface settings

N3 is the user plane interface between the gNodeB and the UPF.

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

Connectivity Settings	Description
<i>IPSec: Select the check box to enable IPsec option.</i>	
Use N2 IPsec Tunnel	This option is available only if IPsec check box is selected on the N2 interface. When this option is selected, the IPSec configuration from the N2 interface will be used for the N3 interface. Otherwise, N3 IPsec configuration is required.
Peer SEG	Select the peer SEG range from the drop-down list.

Connectivity Settings	Description
Destination Port	By default, the destination port is set to 500 and cannot be changed.
Source Port	Set the source port number.
Inner IP Type	Select the IP type: IPv4 or IPv6 .
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to Certificates and cannot be changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	It allows you to upload an archive that contains the certificates and keys for the gNodeB range, using the Upload button. To remove the archive , select the Clear button. The <code>.key</code> and <code>.crt</code> files need to have the same name before extensions.
Use Same Certificates and Private Key For All Tunnels	By default, this option is disabled. Select the toggle button to enable it.
<i>IKE Phase 1</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC , AES-192-CBC , AES-256-CBC , AES-128-GCM-16 , AES-192-GCM-16 , AES-256-GCM-16 .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: NONE . Available options: NONE , HMAC-MD5-96 , HMAC-SHA1-96 , HMAC-MD5-128 , HMAC-SHA1-160 , HMAC-SHA2-256-128 , HMAC-SHA2-384-192 , HMAC-SHA2-512-256 . Restrictions: <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. • If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	Select an option from the drop-down list. Default value: prime256v1(19) . Available options: prime256v1(19) , secp384r1(20) , secp521r1(21) , prime192v1(25) , secp224r1(26) , x25519(31) , x448(32) .

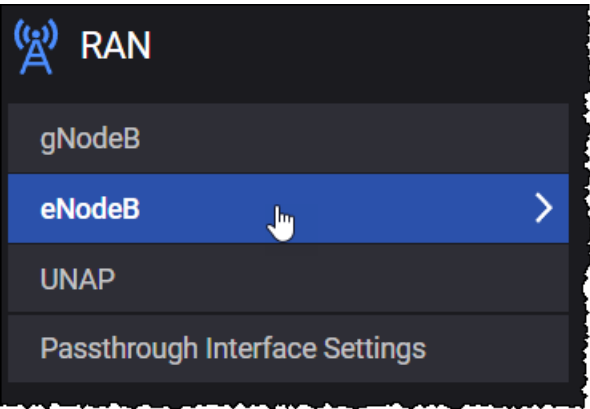
Connectivity Settings	Description
PRF Algorithm	Select an option from the drop-down list. Default value: HMAC-SHA256 . Available options: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512 .
<i>IKE Phase 2</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default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

Connectivity Settings	Description
	Default value: 0 (disabled).
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Emulated Router Address	Set the IPv4 or IPv6 address for the emulated router. This allows to hide all messages from the interface behind a MAC address. <div>NOTE This option can be used only with IxStack stack.</div>
Emulated Router Address Prefix Length	Set the IP network mask for the emulated router.
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
<i>Inner VLAN</i>	<div>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></div> <i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i>

Connectivity Settings	Description
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID..

eNodeB

To configure one or more eNodeB ranges for a test, select **eNodeB** from the RAN panel.



The following topics describe the eNodeB configuration settings:

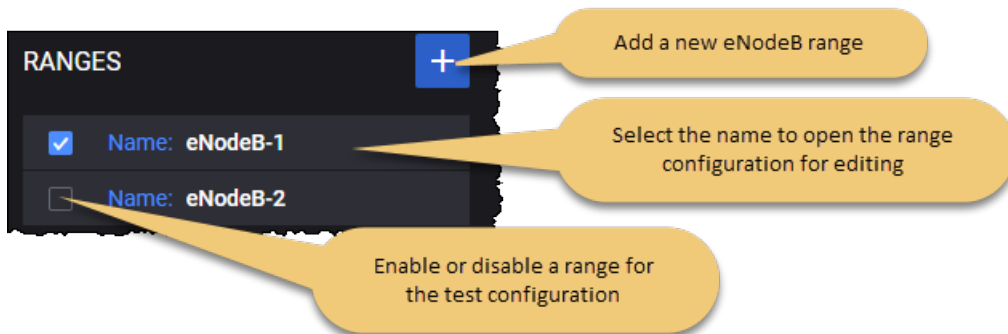
eNodeB Ranges panel	189
eNodeB Range Settings	193
eNodeB Node Settings	194
S1-U Interface Settings	195
S1-MME Interface Settings	196

eNodeB Ranges panel

The **eNodeB Ranges** panel opens when you select the **eNodeB** node from the **RAN** pane. On the Ranges panel, you can perform the following task:

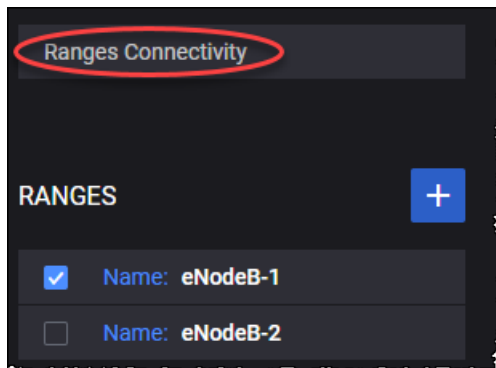
- Add a new eNodeB range to your test configuration.
- Open a eNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



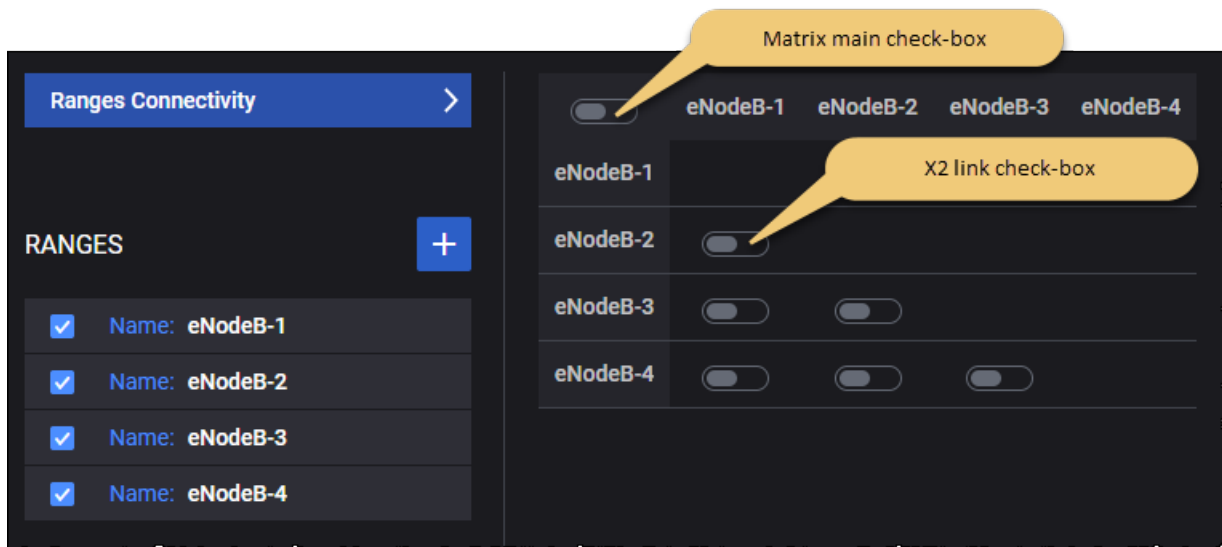
Ranges Connectivity

The Ranges Connectivity section allows you to configure X2 links between eNodeB ranges for handovers. This section is displayed as a matrix of check-boxes, each selected check-box represents an X2 link between ranges on the line and the range on the column.



Note that to configure the X2 links between eNodeB ranges, you need to add at least two eNodeB ranges. If there are fewer than two eNodeB ranges, CoreSIM displays the following message: "Two or more ranges are required to configure X2 links".

Due to the fact that the X2 links are bidirectional the Range Connectivity matrix is only half full of check-boxes.



Each X2 link check-box can have one of the following states:

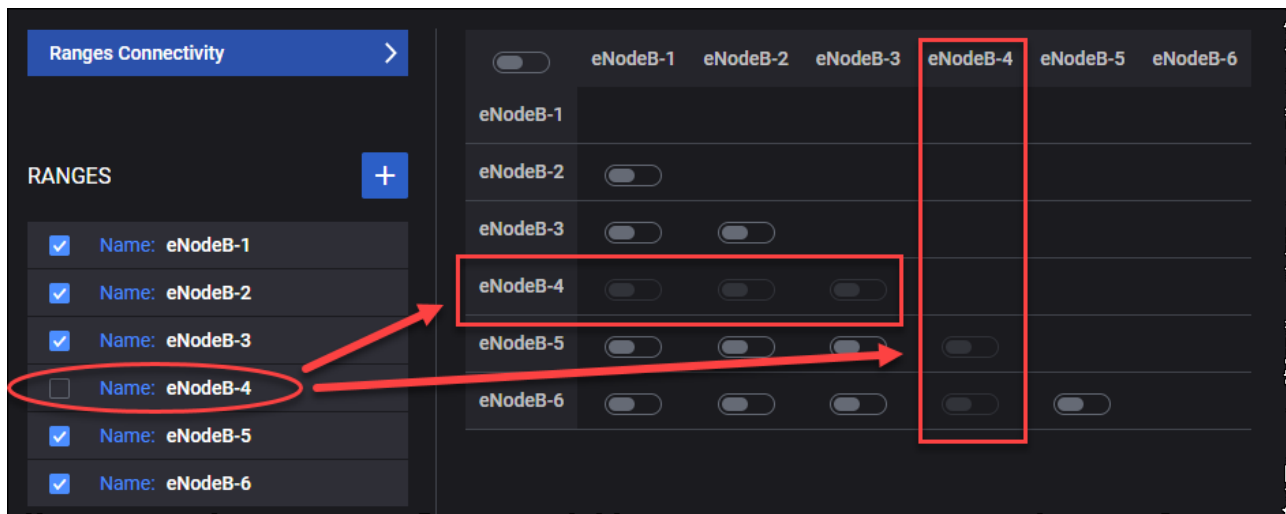
State	Description
Selected and blue color	An X2 link connection is established between enabled eNodeB ranges.
Selected and grey color	An X2 link connection is established between disabled eNodeB ranges.
Unselected	No X2 link connection between eNodeB ranges.

To see all the X2 links for a particular eNodeB range, you need to read the line of that range and then the column of that range.

If none of the links is marked as an X2 link then only S1 handovers will be performed.

Hovering over a specific eNodeB range from the Ranges Connectivity matrix highlights the row and displays more details about the connectivity/range status.

When a eNodeB range is disabled you are not able to select any X2 link for that specific eNodeB range.



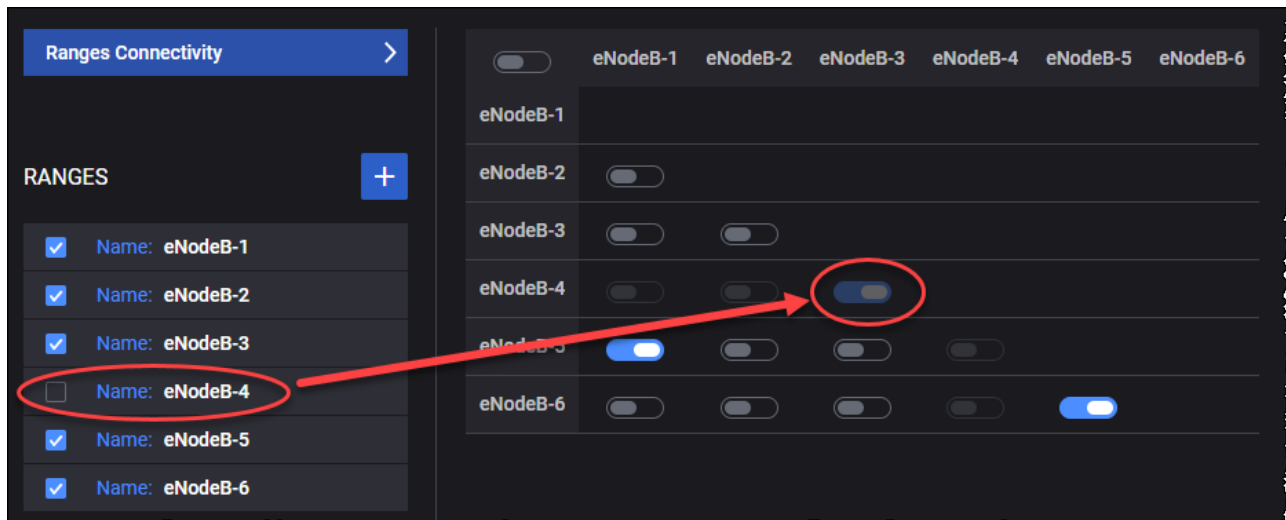
If there was an X2 link between two eNodeB ranges and now one of them is disabled, the check-box will become greyed out and cannot be unselected.

NOTE

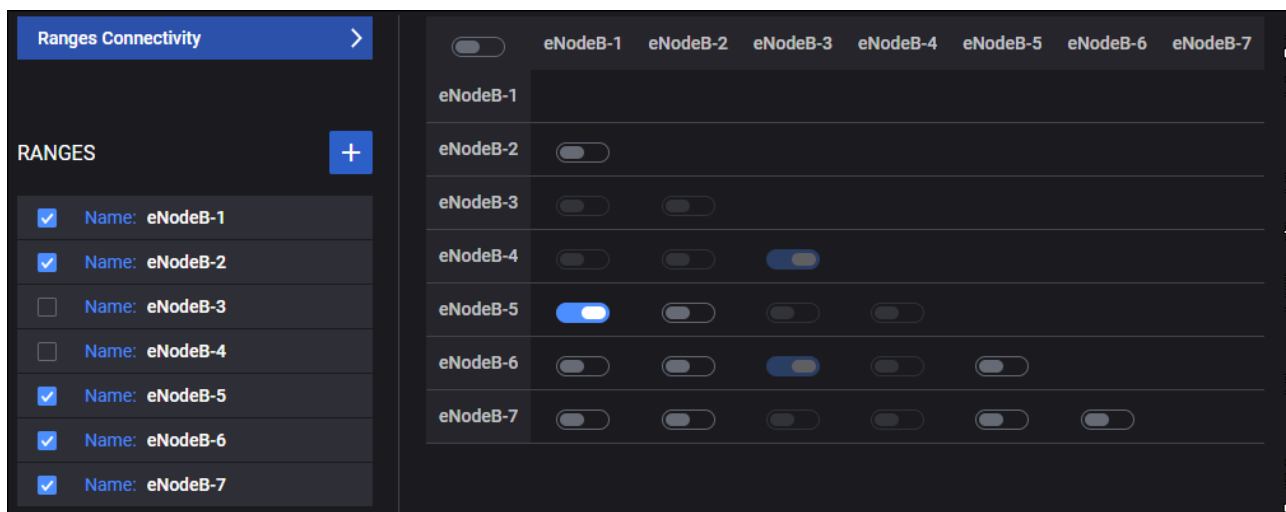
None of the X2 links that are part of disabled eNodeB ranges are sent to the traffic agent.

For example ...

1. The disabled range eNodeB-4 had an X2 link with eNodeB-3. The selected check-box is greyed out. This X2 link will not be sent to the traffic agent.



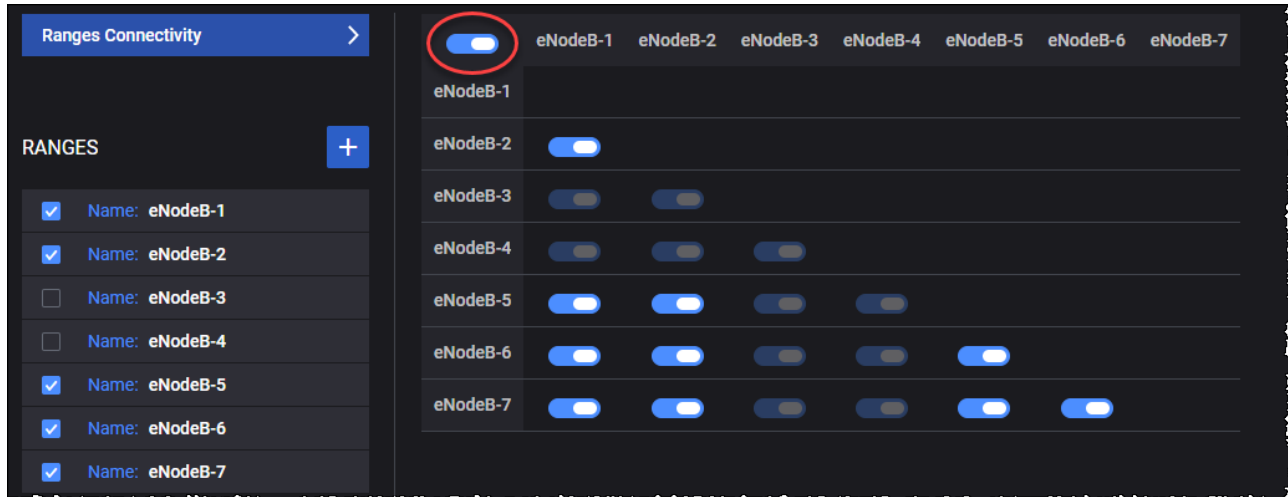
2. The eNodeB-3 range was enabled on previous step and there were selected X2 links between eNodeB-3/eNodeB-4 and eNodeB-3/eNodeB-6. Due to the fact that eNodeB-3 is now disabled, the check-box for X2 links between eNodeB-3 and eNodeB-6 have become greyed out.



The first cell of matrix contains a main check-box that displays the state of the matrix and perform operations.

State	Description	Operation
Selected	All connected.	If the main check-box is Selected, you can undo the selection to change the state to Unselected and all X2 links from the connectivity matrix will become unselected (none connected).
Unselected	None connected.	If the main check-box is Unselected, you can select it to change the state to Checked and all X2 links from the connectivity matrix will become selected (all connected).

When the main matrix check-box is selected all the X2 link check-boxes from the matrix become selected.




Even the X2 link check-boxes for disabled eNodeB ranges are selected since the X2 links for disabled eNodeB ranges are not sent to the traffic agent. This way, when the disabled eNodeB range is enabled, you will not have to manually select the X2 link check-boxes for that particular eNodeB range.

eNodeB Range Settings

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

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

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

eNodeB Node Settings

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

Setting	Description
Name	The name of this eNodeB range. Multiple eNodeB instances (ranges) may be deployed in the test network. Each eNodeB instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by CoreSIM or overwrite it with your own value.
PLMN MCC	The PLMN MCC for this eNodeB range.
PLMN MNC	The PLMN MNC for this eNodeB range.
Tracking area code	The Tracking Area Code to use for the nodes in this range.
eNodeB ID	The eNodeB ID uniquely identifies an eNodeB within a Public Land Mobile Network (PLMN). When the eNodeB <i>Range Count</i> setting is greater than 1, CoreSIM increments the <i>eNodeB ID</i> setting for each eNodeB.
eNodeB ID Length	The number of bits to use for the eNodeB ID. It can have either 20 bits or 28 bits.
Cell ID	The Cell Identifier for this eNodeB range. The Cell Identifier is an 8-bit value that identifies a cell within the eNodeB. The same Cell Identifier is used for each eNodeB defined in a range.
Connection Timeout (ms)	The S1AP connection timeout.
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.

The following parameters are required under the **Public Warning System** pane:

Setting	Description
<i>Public Warning System</i>	<i>Select the check box to enable this option.</i>
PWS Restart Timer (s)	Duration in seconds after which PWS Restart Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38413</i> , 8.9.3 <i>PWS Restart Indication</i> .

Setting	Description
PWS Failure Timer (s)	Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38413</i> , 8.9.4 PWS Failure Indication.

NOTE

If the *Public Warning System* option is enabled and both PWS Restart and PWS Failure procedures are configured to be initiated (non-zero timers), the timers should be different.

S1-U Interface Settings

The **S1-U Interface Settings** should be enabled and configured when the test is simulating the MME and the DUT is an SGW. When CoreSIM simulates the MME and the SGW, these settings should be disabled.

In 4G networks, S1-U is the reference point between the LTE eNodeB and the LTE S-GW. It uses the GTP-U protocol running on top of UDP to provides best-effort data delivery of user datagrams. One GTP tunnel is established for each radio bearer to carry user traffic between the eNodeB and the selected SGW.

Connectivity Settings

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Emulated Router Address	Set the IPv4 or IPv6 address for the emulated router. This allows to hide all messages from the interface behind a MAC address. NOTE This option can be used only with IxStack stack.
Emulated Router Address Prefix Length	Set the IP network mask for the emulated router.
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.

Connectivity Settings	Description
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 <i>MAC Address</i>). The default value is 000000000001.
Outer VLAN	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<div>IMPORTANT</div> 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	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

S1-MME Interface Settings

The **S1-MME Interface Settings** should be enabled and configured when the test is not simulating the MME. When CoreSIM simulates the MME, these settings should be disabled.

In 4G networks, S1 is the interface from the LTE access network (E-UTRAN) to the core network (EPC). It supports a multi-point connection among MMEs/SGWs and eNBs, and comprises two reference points:

- S1-MME: Reference point for the control plane protocol between E-UTRAN and MME.
- S1-U: Reference point between E-UTRAN and SGW for the per bearer user plane tunneling and inter-eNodeB path switching during handover.

S1-MME Interface Settings

In order to run a test using the S1 interface, the eNodeB range must be enabled and configured with a Peer MME.

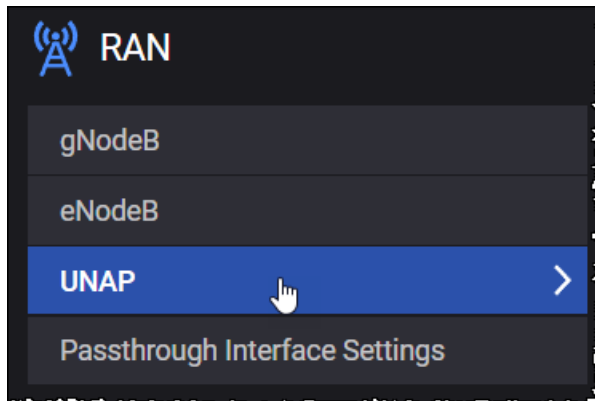
S1 Interface Settings	Description
Peer MME	Select the name of the peer MME node from the drop-down list.
SCTP Source port	The source SCTP port for control plane messages (NG-AP signaling messages). Each SCTP endpoint provides the other endpoint with a list of transport addresses

S1 Interface Settings	Description
	through which that endpoint can be reached and from which it will originate SCTP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP port. The default port number is 36412, but you can change it.
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface. If the <i>Range Count</i> is greater than 1, then this IP Address value is assigned to the first range and is incremented by 1 for each additional range.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
<i>Inner VLAN</i>	<div>IMPORTANT</div> <i>This option is visible only when the Outer VLAN check-box is selected.</i> <i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.

S1 Interface Settings	Description
VLAN TPID	VLAN tag protocol ID.

UNAP

To configure one or more UNAP ranges for a test, select **UNAP** from the RAN panel.



The following topics describe the UNAP configuration settings:

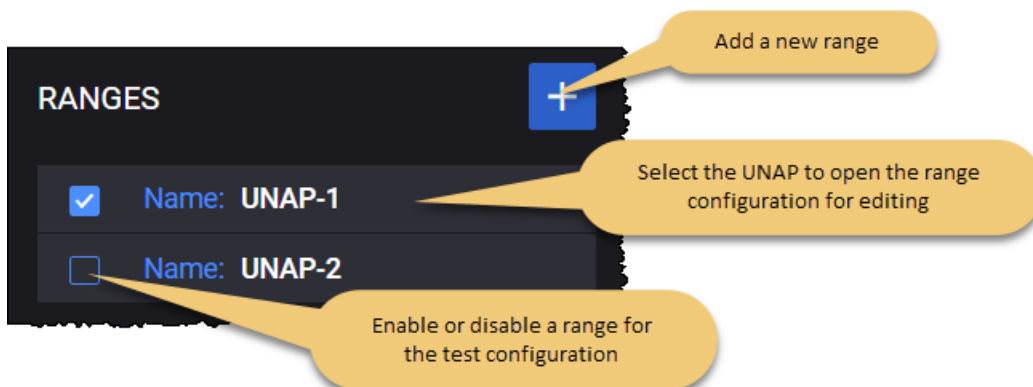
UNAP Ranges panel	198
UNAP Range Settings	199

UNAP Ranges panel

The **UNAP Ranges** panel opens when you select the **UNAP** node from the **RAN** pane. On the Ranges panel, you can perform the following task:

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


For example ...



UNAP Range Settings



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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	
<i>Node Settings</i>	<i>Each UNAP range requires the configuration of an associated set of Node Settings.</i>
Name	The name of this UNAP range. Multiple UNAP instances (ranges) may be deployed in the test network. Each UNAP instance is uniquely identified by its name. You can accept the value provided by CoreSIM or overwrite it with your own value.
UNAP ID	Provide the UNAP identifier value.
UNAP ID Increment	Set the UNAP identifier increment value.
<i>WLAN IP Pool</i>	<i>Each UNAP range requires connectivity settings configuration, which is described below.</i>

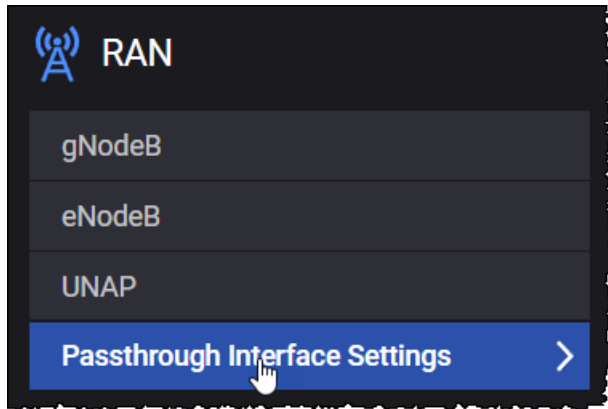
Connectivity Settings

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

Connectivity Settings	Description
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 0.0.0.1.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
<i>Inner VLAN</i>	IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i> <i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

Passthrough interface settings

To configure the passthrough interface settings, select **Passthrough Interface Settings** from the RAN panel.



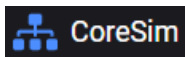
The configuration of the passthrough interface is required when passthrough is enabled in the UE settings. This interface will wait for an external traffic source.

The following settings are required for the passthrough interface configuration.

Connectivity Settings	Description
Stack Type	Select the stack type from the drop-down list. Available options: Single Stack or Dual Stack .
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address assigned as the gateway address for the external traffic source.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
Secondary IP	Select the IP address to open the secondary IP configuration panel for editing. This panel is available only when the stack type is set to Dual Stack .
IP Address	The IP address assigned as the gateway address for the external traffic source.
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	The IP address assigned as gateway address.

Connectivity Settings	Description
Address	
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
MAC	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, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<div>IMPORTANT</div> <p>This option is visible only when the Outer VLAN check-box is selected.</p> <p>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

SEG/N3IWF & CoreSim configuration settings



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

The configuration settings are described in the topics listed below.

Topics:



Core settings	203
N6/SGi interface settings	203
AMF Ranges configuration settings	205
AMF node settings	206
AMF N2 interface settings	210
UPF Ranges configuration settings	211

UPF N3 interface settings	212
MME Ranges configuration settings	213
MME node settings	214
MME S1 interface settings	216
SGW Ranges configuration settings	217
SGW S1-u interface settings	218
SEG Ranges configuration settings	219
SEG interface settings	223
N3IWF Ranges configuration settings	224
N3IWF interface settings	230

Core settings

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

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

Setting	Description
Home Network Private Key	The Home Network Private key that is used for subscriber privacy.
Interworking without N26 interface	When enabled, Core indicates that it supports interworking without N26 interface.
<i>Routing Indicators</i>	<p><i>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.</i></p> <p><i>You can add as many Routing Indicators as necessary to support your test objectives.</i></p>
	Select the Add Routing Indicator button to add a Routing Indicator.
	Select the Delete button to remove the routing indicator.

N6/SGi interface settings

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

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

Connectivity Settings	Description
Stack Type	Select the stack type from the drop-down list. Available options: Single Stack or Dual Stack .
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	Maximum transmission unit.
MSS	Maximum segment size.
<i>Secondary IP</i>	<i>Select the IP address to open the secondary IP configuration panel for editing. This panel is available only when the stack type is set to Dual Stack.</i>
IP Address	The IP address assigned as the gateway address for the external traffic source.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

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

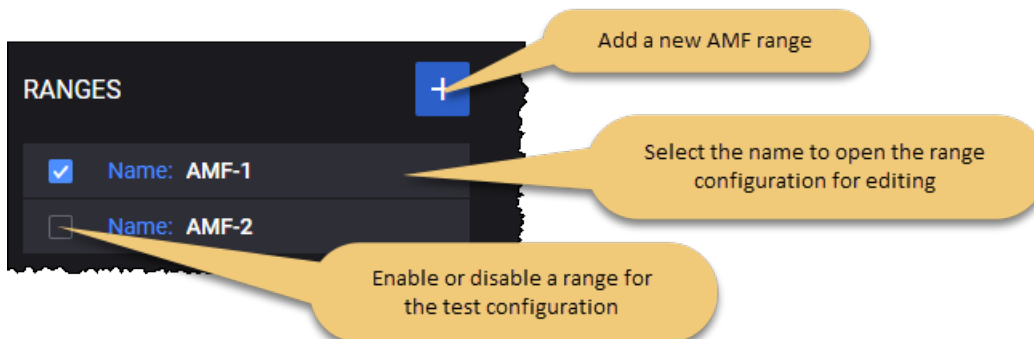
AMF Ranges configuration settings

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

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

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

For example ...



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


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

AMF range controls and settings

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

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

Setting	Description
Range:	

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

AMF node settings

Each AMF range includes a set of Node Settings.

Node Settings

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



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

Setting	Description
	Subscriber Identity)), and is also used in combination with the MCC to identify a PLMN.
Region ID	<p>An AMF Region consists of one or multiple AMF Sets.</p> <p>The AMF Region ID to use for this simulated AMF node. This ID identifies the region in which the node resides. The AMF Region ID addresses the case that there are more AMFs in the network than the number of AMFs that can be supported by AMF Set ID and AMF Pointer. It allows operators to re-use the same AMF Set IDs and AMF Pointers in different regions.</p>
Set ID	<p>An AMF Set consists of some AMFs that serve a given area and Network Slice. Multiple AMF Sets may be defined per AMF Region and Network Slice(s).</p> <p>The AMF Set ID to use for this simulated AMF node. The Set ID uniquely identifies the AMF Set within the AMF Region.</p>
Pointer	The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.
Relative Capacity	Set the relative capacity value.
Ciphering Algorithm	<p>Allows to select the supported 5G ciphering algorithm:</p> <ul style="list-style-type: none"> • NEA0 - Null ciphering algorithm • NEA1 - 128-bit SNOW 3G based algorithm • NEA2 - 128-bit AES based algorithm • NEA3 - 128-bit ZUC based algorithm
Integrity Algorithm	<p>Allows to select the supported 5G integrity protection algorithm:</p> <ul style="list-style-type: none"> • NIA0 - Null Integrity Protection algorithm • NIA1 - 128-bit SNOW 3G based algorithm • NIA2 - 128-bit AES based algorithm • NIA3 - 128-bit ZUC based algorithm
Request N2 SM Information	Enable this option to request N2 SM Information again instead of using the existing one.
Prefer AMF Change	Enable this option to change the AMF for an N2 handover even when the target RAN(T-RAN) is connected to the serving AMF.
Skip MT SMS	Enable this option to skip the initiation of MT SMS procedure when the MO SMS procedure ends.
<p><i>T3512: Select the check box to open T3512 Settings and configure the T3512 timer.</i></p> <div> <div>NOTE</div> <div><i>If disabled, a value of 50 minutes (Value 5 X Unit 10 minutes) is sent for T3512.</i></div> </div>	

Setting	Description
Value	Set the value for this parameter. The accepted values are between 0-31.
Unit	Select the unit size for this parameter from the drop-down list. The available options are: 2s, 30s, 1m, 10m, 1h, 10h and Deactivated.
NSSAI	<i>These settings are described below.</i>
TAI	<i>These settings are described below.</i>
Public Warning System	<i>These settings are described below.</i>
Emergency Settings	<i>These settings are described below.</i>





NSSAI

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

Setting	Description												
NSSAI:													
	Select the Add NSSAI button to add a new NSSAI to your test configuration.												
NSSAI settings:													
	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 NSSAI information element. The standardized SST values are:												
	<table><tr><th>SST</th><th>Value</th><th>Suitable for handling:</th></tr><tr><td>eMBB</td><td>1</td><td>5G enhanced Mobile Broadband</td></tr><tr><td>URLCC</td><td>2</td><td>ultra-reliable low-latency communications</td></tr><tr><td>MIoT</td><td>3</td><td>massive IoT</td></tr></table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
	SST	Value	Suitable for handling:										
	eMBB	1	5G enhanced Mobile Broadband										
	URLCC	2	ultra-reliable low-latency communications										
MIoT	3	massive IoT											
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the NSSAI.												

TAI

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

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

Public Warning System

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

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

Emergency Settings

The following table describes the emergency settings configuration.

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

AMF N2 interface settings

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

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

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix that has been assigned to this node.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.

Connectivity Settings	Description
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, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<div>IMPORTANT</div> 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	VLAN identifier.

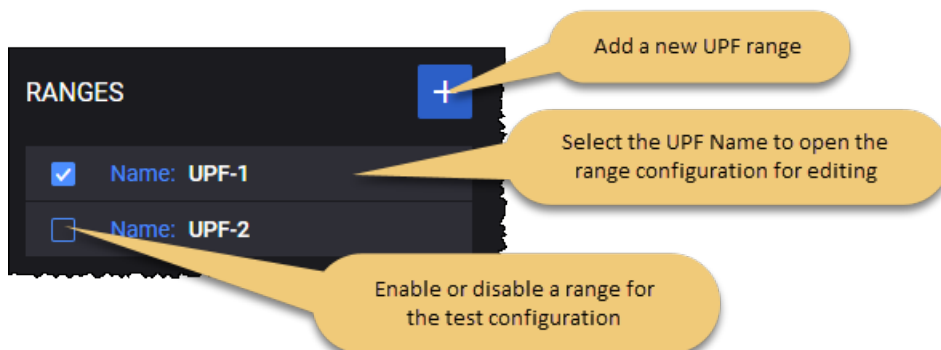
UPF Ranges configuration settings

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

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

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


For example ...



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

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

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

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

UPF N3 interface settings

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

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

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

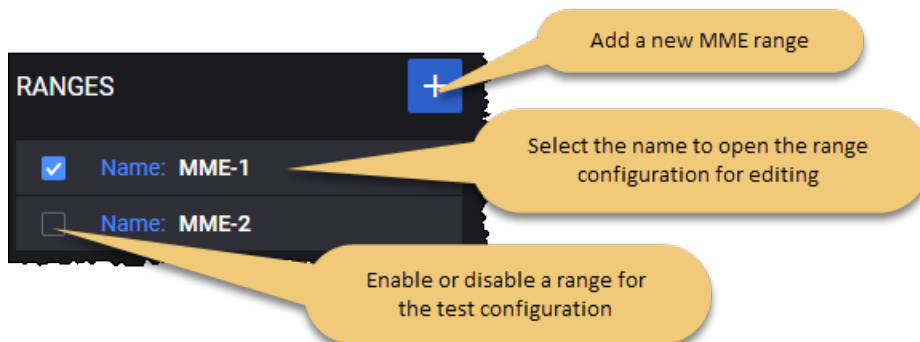
MME Ranges configuration settings

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

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

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

For example ...



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


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

MME range controls and settings

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

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

Setting	Description
Range:	

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

MME node settings

Each MME range includes a set of Node Settings.

Node Settings

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

Setting	Description
<i>Node Settings:</i>	
Name	The name uniquely identifies each MME instance. You can accept the value provided by CoreSIM or overwrite it with your own value.
Group ID	Set the MME group ID value.
Code	Set the MME code value.
PLMN MCC	<p>The PLMN MCC for this MME range.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this MME range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>

Setting	Description
Ciphering Algorithm	Allows to select the supported 5G ciphering algorithm: <ul style="list-style-type: none"> • EEA0 - Null ciphering algorithm • EEA1 - 128-bit SNOW 3G based algorithm • EEA2 - 128-bit AES based algorithm • EEA3 - 128-bit ZUC based algorithm
Integrity Algorithm	Allows to select the supported 5G integrity protection algorithm: <ul style="list-style-type: none"> • EIA0 - Null Integrity Protection algorithm • EIA1 - 128-bit SNOW 3G based algorithm • EIA2 - 128-bit AES based algorithm • EIA3 - 128-bit ZUC based algorithm
Relative Capacity	Set the relative capacity value.

Public Warning System

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

Setting	Description
<i>Public Warning System</i>	<i>Select the check box to enable this option.</i>
Message ID	Set the public warning system message ID. Values should be in range 0-65535. Default value: 4352 .
Repetition Period	Set the public warning system message repetition period. Values should be in range 1-131071. Default value: 1 .
Number of Broadcasts Requested	Set the public warning system message number of requested broadcasts. Values should be in range 0-65535. Default value: 1 .
Time to Wait Before Triggering PWS after NG Setup (s)	Set the number of seconds to wait before triggering PWS after S1 setup. Values should be in range 0-86400. Default value: 1 .
PWS Kill Timer (s)	Duration in seconds after which PWS Kill Request is sent. Values should be in range 0-86400. Default value: 0 .

MME S1 interface settings

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

S1 Interface Settings	Description
Local STCP Port	Set the local STCP port number.
<i>Connectivity Settings</i>	
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
<i>Inner VLAN</i>	<div>IMPORTANT</div> <i>This option is visible only when the Outer VLAN check-box is selected.</i> <i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i>

S1 Interface Settings	Description
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

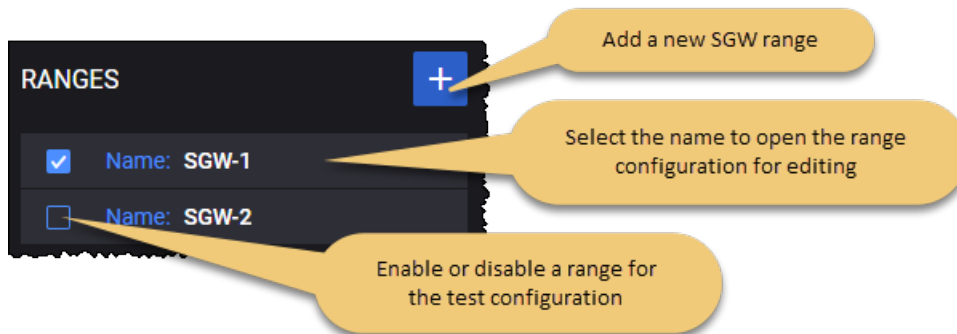
SGW Ranges configuration settings

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

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

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

For example ...




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

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

SGW range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Name	The name uniquely identifies each SGW instance. You can accept the value

Setting	Description
	provided by CoreSIM or overwrite it with your own value.
<i>Range Settings:</i>	
UDP Rx Buffer (bytes)	Size of receive buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 #The default Linux buffer size • maximum: 134217728 #128MB • default: 12582912 #12MB
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 # The default Linux buffer size • maximum: 134217728 #128MB • default: 2097152 #2MB
S1-u Interface Settings	These settings are described in SGW S1-u interface settings .

SGW S1-u interface settings

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

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

S1-u Interface Settings	Description
	<i>VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<div>IMPORTANT</div> <i>This option is visible only when the Outer VLAN check-box is selected.</i> <i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

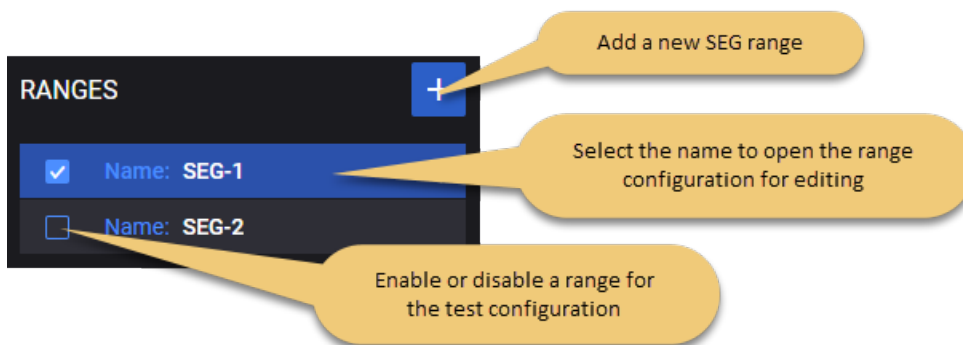
SEG Ranges configuration settings

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

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

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

For example ...




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

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

SEG range controls and settings

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

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

Setting	Description
<i>Range:</i>	
Device Under Test	Enable this option if your SEG is a DUT in this test configuration. When this option is not enabled, the CoreSIM will simulate the SEG functionality (if it is selected in the Topology window).
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	
<i>Node Settings</i>	
Name	The name uniquely identifies each SGW instance. You can accept the value provided by CoreSIM or overwrite it with your own value.
Role	By default, the role is set to Responder (Remote Access) and cannot be changed.
UDP Rx Buffer (bytes)	Size of receive buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 12582912
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 2097152
<i>Interface Settings</i>	<i>These settings are described in SEG interface settings.</i>
<i>Remote Access IP Pool</i>	
Start IP	Set the start IP address.
IP Increment	Set the IP address increment value.
IPs count	Set the IP count value.
IP Prefix Length	Set the IP prefix length value.

Setting	Description
<i>Local Protected Subnet</i>	<i>Selects which node(s) are protected by SEG: AMF and/or UPF . AMF and UPF could be protected by the same SEG when running with Linux stack.</i>
N2 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific AMF range from the list.
N3 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific UPF range from the list.
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to Certificates and cannot be changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	It allows you to upload an archive that contains the certificates and keys for the SEG range, using the Upload button. To remove the archive , select the Clear button. The <code>.key</code> and <code>.crt</code> files need to have the same name before extensions.
Use Same Certificates and Private Key For All Tunnels	By default, this option is disabled. Select the toggle button to enable it.
<i>IKE Phase 1</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC , AES-192-CBC , AES-256-CBC , AES-128-GCM-16 , AES-192-GCM-16 , AES-256-GCM-16 .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: NONE . Available options: NONE , HMAC-MD5-96 , HMAC-SHA1-96 , HMAC-MD5-128 , HMAC-SHA1-160 , HMAC-SHA2-256-128 , HMAC-SHA2-384-192 , HMAC-SHA2-512-256 . Restrictions: <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. • If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	Select an option from the drop-down list. Default value: prime256v1(19) . Available options: prime256v1(19) ,

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

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

SEG interface settings

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

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

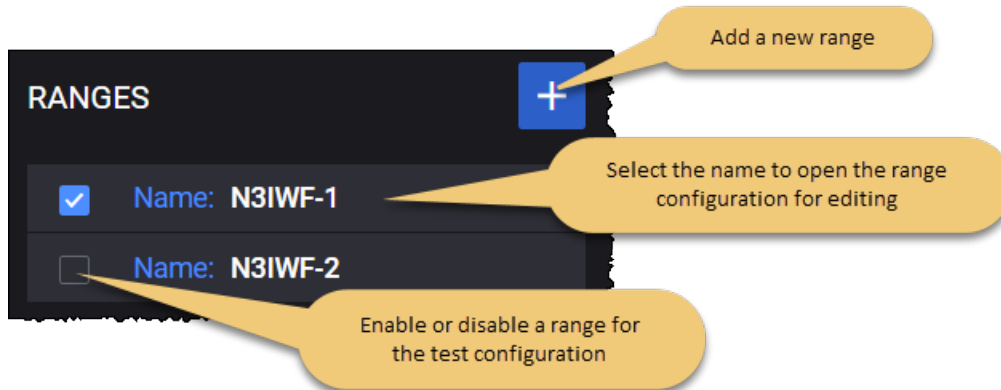
N3IWF Ranges configuration settings

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

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

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

For example ...




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

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

N3IWF range controls and settings

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

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

Setting	Description
<i>Range:</i>	
Device Under Test	Enable this option if your N3IWF is a DUT in this test configuration. When this option is not enabled, the CoreSIM will simulate the N3IWF functionality (if it is selected in the Topology window).
	Select the Delete Range button to delete this range from your test configuration.
<i>Range Settings:</i>	

Setting	Description
<i>Node Settings</i>	
Name	The name uniquely identifies each N3IWF instance. You can accept the value provided by CoreSIM or overwrite it with your own value.
Role	By default, the role is set to Responder (Remote Access) and cannot be changed.
PLMN MCC	<p>The PLMN MCC for this N3IWF range.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this N3IWF range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Tracking Area Code	Provide the Tracking Area Code (TAC) value
N3IWF ID	Set the value for this field.
N3IWF ID Increment	Set the increment value for this field.
SCTP Tx Buffer (bytes)	Set the size of SCTP Tx Buffer.
SCTP Rx Buffer (bytes)	Set the size of SCTP Rx Buffer.
UDP Rx Buffer (bytes)	<p>Size of receive buffers for UDP sockets:</p> <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 12582912

Setting	Description
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 2097152
<i>Traffic Profiles</i>	<i>These settings are described in Traffic Profiles settings.</i>
<i>NSSAI</i>	<i>These settings are described in NSSAI settings.</i>
<i>NWu Interface Settings</i>	<i>These settings are described in N3IWF interface settings.</i>
<i>N2 Interface Settings</i>	<i>These settings are described in N3IWF interface settings.</i>
<i>N3 Interface Settings</i>	<i>These settings are described in N3IWF interface settings.</i>
<i>Remote Access IP Pool</i>	
Start IP	Set the start IP address.
IP Increment	Set the IP address increment value.
IPs count	Set the IP count value.
IP Prefix Length	Set the IP prefix length value.
<i>Local Protected Subnet</i>	<i>Selects which node(s) are protected by SEG: AMF and/or UPF . AMF and UPF could be protected by the same SEG when running with Linux stack.</i>
N2 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific AMF range from the list.
N3 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific UPF range from the list.
<i>Authentication</i>	
Configure Certificates	By default, this option is disabled. When enabled, the following fields needed to add certificates became available.
Certificates (.zip)	It allows you to upload an archive that contains the certificates for the N3IWF range, using the Upload button. To remove the archive , select the Clear button.
Use Same Certificates For	By default, this option is disabled. Select the toggle button to enable it.

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

Setting	Description
	<ul style="list-style-type: none"> If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	Select an option from the drop-down list. Default value: ID_DER_ASN1_DN . Available options: ID_IPV4_ADDR , ID_FQDN , ID_USER_FQDN , ID_IPV6_ADDR , ID_DER_ASN1_DN , ID_KEY_ID .
Local Identification Value	Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN , ID_KEY_ID or ID_RFC822_ADDR .
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: 0 (disabled).

Traffic Profiles

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

NOTE Only one Control Plane Profile is accepted.



Setting	Description
TCP Port	The TCP port for N3IWF: <ul style="list-style-type: none"> default value: 20000. minimum value: 1024. maximum value: 65535.
IP Type	Select the IP type from the drop-down list: IPv4 (default) or IPv6 .
Local Protected Subnet IP Address	The IP address for N3IWF TCP server.

Setting	Description
	Default value: 150.0.2.1 .
Local Protected Subnet IP Prefix Length	The only accepted options are 32 for IPv4 and 128 for IPv6.
Remote Inner IP Address	Per UE IP Address used for TCP Control Plane connection. Address increment is 1. Default value: 150.0.100.1 .

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


NOTE


A maximum of 15 Control Plane Profile can be configured.

Setting	Description
	Select the Add User Plane button to add a new profile to your test configuration.
	Select the Delete User Plane button to delete this profile from your test configuration.
DNN	Select the DNN value for the drop-down list.
IP Type	Select the IP type from the drop-down list: IPv4 (default) or IPv6 .
Local Protected Subnet IP Address	The IP address for N3IWF GRE endpoint. Default value: 150.1.2.1 .
Local Protected Subnet IP Prefix Length	The only accepted options are 32 for IPv4 and 128 for IPv6.
Remote Inner IP Address	Per PDU Session IP Address used for GRE User Plane connection. Address increment is 1. Default value: 150.1.100.1 .

NSSAI

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

Setting	Description
<i>NSSAI:</i>	
	Select the Add NSSAI button to add a new NSSAI to your test configuration.
<i>NSSAI settings:</i>	


Setting	Description												
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.												
SST	<div>The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:</div> <table><tr><th>SST</th><th>Value</th><th>Suitable for handling:</th></tr><tr><td>eMBB</td><td>1</td><td>5G enhanced Mobile Broadband</td></tr><tr><td>URLCC</td><td>2</td><td>ultra-reliable low-latency communications</td></tr><tr><td>MIoT</td><td>3</td><td>massive IoT</td></tr></table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
SST	Value	Suitable for handling:											
eMBB	1	5G enhanced Mobile Broadband											
URLCC	2	ultra-reliable low-latency communications											
MIoT	3	massive IoT											
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the NSSAI.												


N3IWF interface settings

NWu interface settings

The following settings enable connectivity and service interaction.

Interface Settings	Description
Source Port	Set the source port number.

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.



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

N2 interface settings

The following settings enable connectivity and service interaction.

Interface Settings	Description
Peer AMF	The IP address of the AMF node connected over the N2 interface.
Destination port	The destination Stream Control Transmission Protocol (SCTP) port for control plane messages (NG-AP signaling messages) on the N2 interface.
SCTP source port	The source SCTP port for control plane messages (NG-AP signaling messages). Each SCTP endpoint provides the other endpoint with a list of transport addresses through which that endpoint can be reached and from which it will originate SCTP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP port. The default port number is 36412, but you can change it.



Interface Settings	Description
Connection Timeout (ms)	Set the connection timeout value.
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum Retransmission Timeout (ms)	Set the maximum retransmission timeout value, in milliseconds.
Initial Retransmission Timeout (ms)	Set the initial retransmission timeout value, in milliseconds.
Maximum Retransmission per Association	Set the maximum retransmissions value per association.
Maximum Retransmission per Path	Set the maximum retransmissions value per path.
Heartbeat Interval (ms)	Set the heartbeat interval value, in milliseconds.
SACK Delay (ms)	Set the delayed selective ACK timeout value.
SACK Frequency	Set the delayed selective ACK frequency value.
Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.

Connectivity Settings	Description
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Emulated Router Address	Set the IPv4 or IPv6 address for the emulated router. This allows to hide all messages from the interface behind a MAC address. NOTE This option can be used only with IxStack stack.
Emulated Router Address Prefix Length	Set the IP network mask for the emulated router.
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
<i>Inner VLAN</i>	IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i>

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

N3 interface settings

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

SEG Interface Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.

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

CHAPTER 7

Manage and use test sessions

When you create a new test, CoreSIM 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:

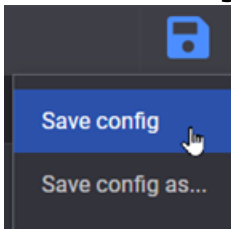
Save test sessions	236
Manage test sessions	237
Import and export sessions	239
Delete configs and sessions	240

Save test sessions

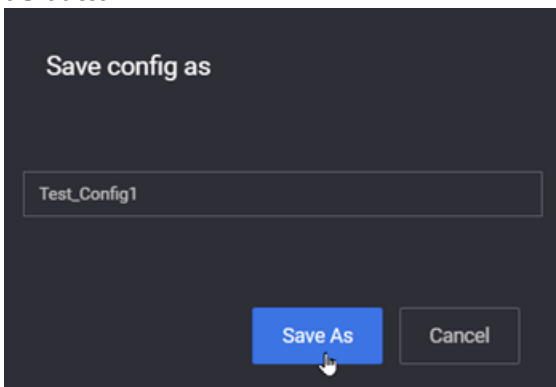
Once a test is configured, you can record its configuration as a session, edit and save it for future use.

To save a configuration file, do the following:

1. Click the **Save** icon from the upper-right corner of the **Test Overview** page.
2. Click **Save config** to quickly save your test configuration.

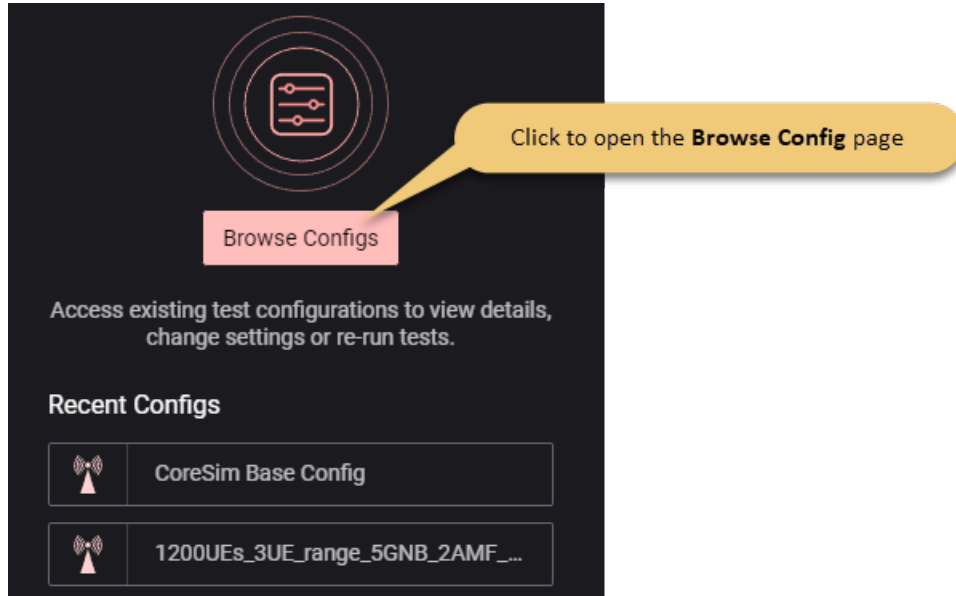


3. Click **Save config as** to save your test configuration with a specific name.
4. Provide the name for the test configuration in the **Save config as** window and click the **Save as** button.



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 CoreSIMDashboard.



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 facing page](#)
- [Manage configurations on the facing page](#)

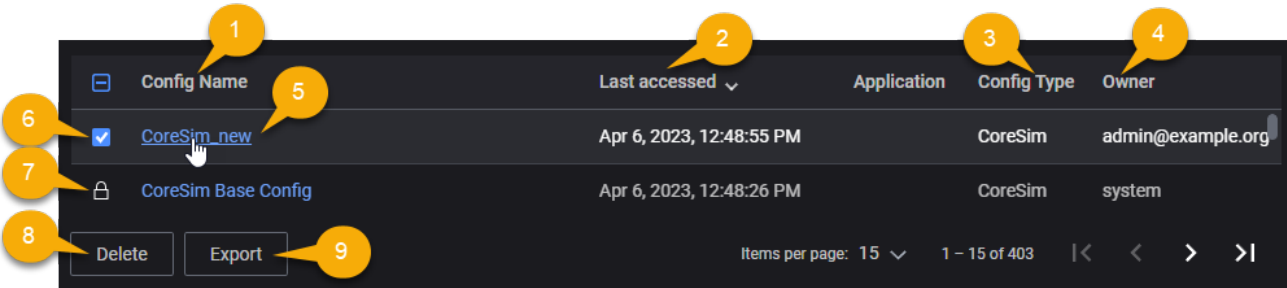
View configuration categories

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



Manage configurations

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



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 name link. You can open the current session from here or can create a new session based on this configuration.
6	Use to select a test configuration.
7	Indicates a base configuration <div>NOTE For the base configurations, the test owner is <i>system</i>.</div>
8	Click the button to delete the test configuration.
9	Click the button to export the test configuration.

Import and export sessions

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

If you want to export only a specific configuration, select it from the configuration list and select [Export](#).

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.

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.

<input type="checkbox"/>	Config Name	Last accessed ▾	Application	Config Type	Owner
<input type="checkbox"/>	CoreSim_new (copy from Apr 6 10:06:49)	Apr 6, 2023, 1:06:49 PM		CoreSim	admin@exascale.com
<input type="checkbox"/>	CoreSim_new	Apr 6, 2023, 12:48:55 PM		CoreSim	admin@exascale.com
<input type="checkbox"/>	CoreSim Base Config			CoreSim	system

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 CoreSIM 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.

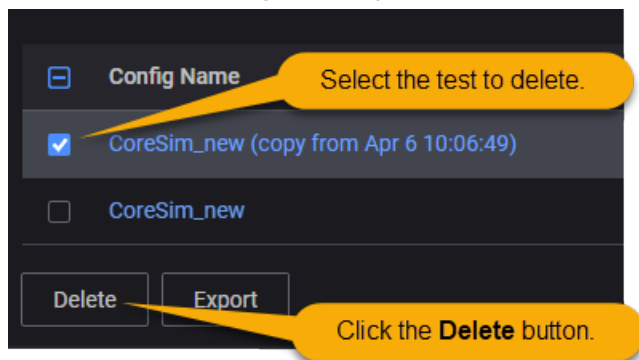
Delete configs and sessions

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 CoreSIM 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.



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

Important notes

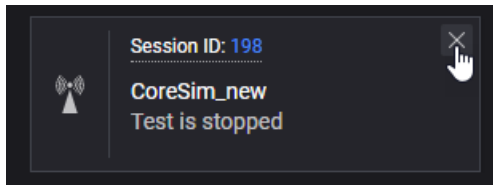
Before deleting a session, be aware of the following application behaviors:

- 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 2.0 session

You can also delete a test session from the Dashboard:

1. Go to the **Dashboard**.
2. Locate the tile for the session that you plan to delete, then click the **X** in the upper right corner. CoreSIM opens a confirmation dialog.



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

CHAPTER 8

Manage CoreSIM licenses

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

Chapter contents:

Licensing Requirements	242
License Manager	242
License Server	244

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 CoreSIM web UI.

License Manager

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

- [How to open License Manager on the next page](#)
- [Activate a license on the next page](#)
- [Deactivate a license on the next page](#)
- [Sync licenses on the next page](#)
- [Reserve a license on the next page](#)
- [Get license statistics on page 244](#)
- [Perform offline license operations on page 244](#)

How to open License Manager

To access the CoreSIM License Manager:

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

Activate a license

To activate one or more CoreSIM licenses:

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

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

Deactivate a license

To deactivate one or more CoreSIM 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.

NOTE

It is recommended to deactivate the license before deleting a CoreSIM VM. This way you can easily reuse the same license (Activation Code) when deploying another CoreSIM VM.

Sync licenses

To synchronize one or more CoreSIM licenses:

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

Reserve a license

To reserve one or more CoreSIM licenses:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select the **Manage Reservation** icon.
CoreSIM 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 CoreSIM 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 CoreSIM license operations:

1. Select **Administration** from the setup menu (⚙️), then select **License Manager**.
2. Select **Offline operations**.
CoreSIM 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 CoreSIM 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 CoreSIM web UI:

1. Log in the CoreSIM 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 CoreSIM web UI:

1. Log in the CoreSIM 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 CoreSIM licenses:

1. From the Setting menu () , select **Application Settings**.
CoreSIM 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 9

Manage CoreSIM users

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

User categories

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

1. Select the settings menu (⚙️) and then select **Administration**.
2. Select **Access Control** from the **Administration** menu.
CoreSIM opens the **Keycloak Admin Console** in a new browser tab.
3. Select **Users** from the list of **Manage** functions (in the navigation pane).
4. Select the **Add user** button.
5. 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**.
6. Select the **Save** button.
CoreSIM adds the user and displays that user's information in the **Details** tab.
7. 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.

CoreSIM 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 **Administration**.
2. Select **Access Control** from the **Administration** menu.
CoreSIM opens the **Realm Settings** window.
3. Select **Users** from the list of **Manage** functions.
4. Select the user.
5. Select the **Credentials** tab.
6. Enter the new *Password*.
7. Re-enter the new password in the *Password Confirmation* field.
8. Set *Temporary* **ON** if the user will be required to change the password upon initial log in.
9. Select the **Reset Password** button.
CoreSIM displays a confirmation dialog.
10. Select the **Reset Password** button to confirm the action.

Disable a user account

Administrative users can temporarily disable a user's account:

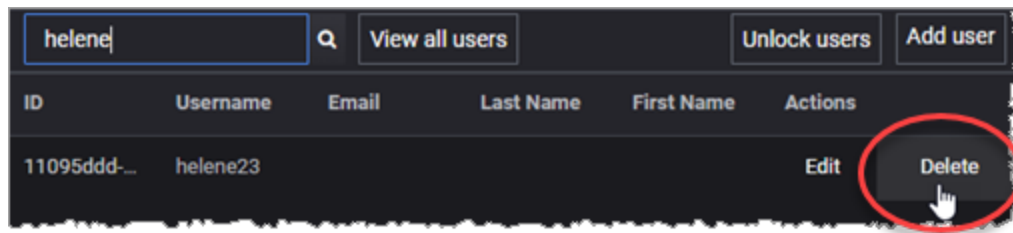
1. Select the settings menu (⚙️) and then select **Administration**.
2. Select **Access Control** from the **Administration** menu.
CoreSIM opens the **Realm Settings** window.
3. Select **Users** from the list of **Manage** functions.
4. Select the user.
5. Set *User Enabled* to **OFF**.

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 **Administration**.
2. Select **Access Control** from the **Administration** menu.
CoreSIM opens the **Realm Settings** window.
3. Select **Users** from the list of **Manage** functions.
4. View all users or search for the Username of the account that you will delete.
5. Click **Delete**.



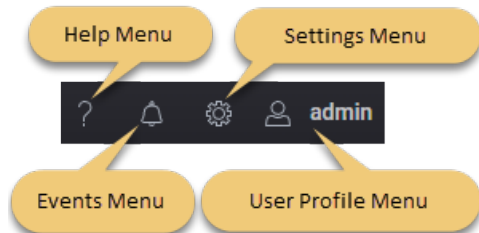
6. CoreSIM opens a confirmation dialog.
7. Select **Delete** to confirm that you are permanently deleting this user account.

This page intentionally left blank.

CHAPTER 10

CoreSIM general settings

The **Settings** menu can be accessed by selecting the gear icon (⚙️) on the top right corner of the **Dashboard** page.



It contains the following menus:

- [Help](#)
- [Events](#)
- [Settings](#)
- [User Profile](#)

Help Menu

The **Help Menu** can be accessed by selecting the question mark icon on the top right corner of the Dashboard page. Here you can do the following actions:

- Access **Help** where you can find info about the official CoreSIM documentation and access the Rest API Browser.
- Access **Technical Support** section, where you can do the following:
 - **Contact Keysight**
 - **Collect diagnostics** - for more details refer to [Collect Diagnostics](#).
 - **EULA** - select this option to revisit and accept Keysight Software End User License agreement.
 - Access **My software support...** for official Keysight support.
 - **About** - this option displays details regarding the running software version.

Events Menu

The **Events Menu** can be accessed by selecting the bell icon on the top right corner of the Dashboard page. You can [view notifications and test events](#).

Settings Menu

The **Settings Menu** can be accessed by selecting the wheel icon on the top right corner of the Dashboard page. Here you can do the following actions:

- **License Manager** - select this option to open the [License Manager](#) section.
- **Agent Management** - select this option to open the Traffic agents management section.

- **Software Updates** - select this option to open the Software Updates section. To update to a newer version, do the following:
 - Open the **Settings** menu (⚙️) and click on **Software Updates**.
 - Click **Select Packages For Upload** and open the folder containing the upgrade file.
 - Select the upgrade file and click **Open**.
 - Click **Start Update** to initiate the update process.
 - If needed, you can remove the update packages from the update section by clicking **Reset Current Changes**.
- **Application settings** - select this option set or update the license server IP. For more details, refer to [Configure License Server](#).
- **Logs Level** - select this option to collect logs info. For more details, refer to [Collect Diagnostics, Cleanup and Data Migration](#).
- **Data migration** - select this option to open the data migration tool. For more details, refer to [Collect Diagnostics, Cleanup and Data Migration](#).
- **System Monitor** - select this option to open the system tool. For more details, refer to [Collect Diagnostics, Cleanup and Data Migration](#).
- **User Management** - select this option to open the [Access Control](#) section. This section handles server administration security configuration and also all the users settings. For more information on the Access Control options and configuration, refer to the official [Keycloak documentation](#).

User Profile

The **User Profile Menu** can be accessed by selecting the user icon on the top right corner of the Dashboard page. Here you can:

- Access and review your user profile.
- Change CoreSIM Dashboard theme.
- **Log Out** - select this option to log out of CoreSIM.

CHAPTER 10

Statistics

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.

NOTE

CoreSIM 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.

This page intentionally left blank.

CHAPTER 11

Troubleshooting

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

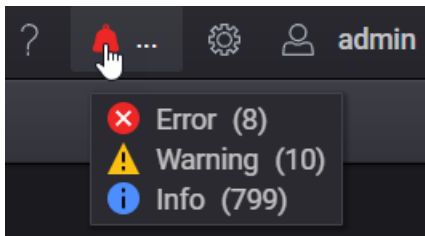
Chapter contents:

View Notifications and Test Events	254
Collect Diagnostics, Cleanup and Data Migration	256
NTP troubleshooting	259

View Notifications and Test Events

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

When a notification is triggered, a color-coded banner is displayed when you hover over the notification icon:






- **Blue** - for informational messages
- **Orange** - for messages informing you of actions you are not allowed to perform
- **Red** - for error messages







Types of events:

- **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.
- **INFO** - An *info* notification indicates a general-purpose notification, such as logging data or a heartbeat indicator.
- **WARNING** - A *warning* notification indicates an error has occurred that potentially impacts application stability.

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

Events

☒ All ☒  Info ☒  Warning ☒  Error

Date ▾	Type	Message
Apr 11, 2023, 9:41:39 AM	 ERROR	PDF report generation failed
Apr 11, 2023, 9:41:37 AM	 INFO	Generating PDF report for wireless-566c8b5a-47a6-41ba-b0bf-5602...
Apr 11, 2023, 3:04:06 AM	 INFO	Sessions configs upgraded successfully. Refresh is needed on GUI.
Apr 11, 2023, 3:04:01 AM	 INFO	A new ATI Updates version was installed. The new version is 23.3.33.
Apr 11, 2023, 3:03:39 AM	 INFO	Update finished successfully
Apr 10, 2023, 7:07:23 PM	 INFO	[Throughput 10G] Acquired 1 WRLS-5GC-UPTPUT-10G licenses for t...

[Go to events page](#) [Close](#)

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.

Home > Events

Filter events by

Message:

Date: To

Notification type: ☒ All ☒ Info ☒ Warning ☒ Error

Date	Type	Message
Apr 11, 2023, 9:41:39 AM	ERROR	PDF report generation failed
Apr 11, 2023, 9:41:37 AM	INFO	Generating PDF report for wireless-566c8b5a-47a6-41ba-b0bf-56021902eb01.
Apr 11, 2023, 3:04:06 AM	INFO	Sessions configs upgraded successfully. Refresh is needed on GUI.
Apr 11, 2023, 3:04:01 AM	INFO	A new ATI Updates version was installed. The new version is 23.3.33.
Apr 11, 2023, 3:03:39 AM	INFO	Update finished successfully

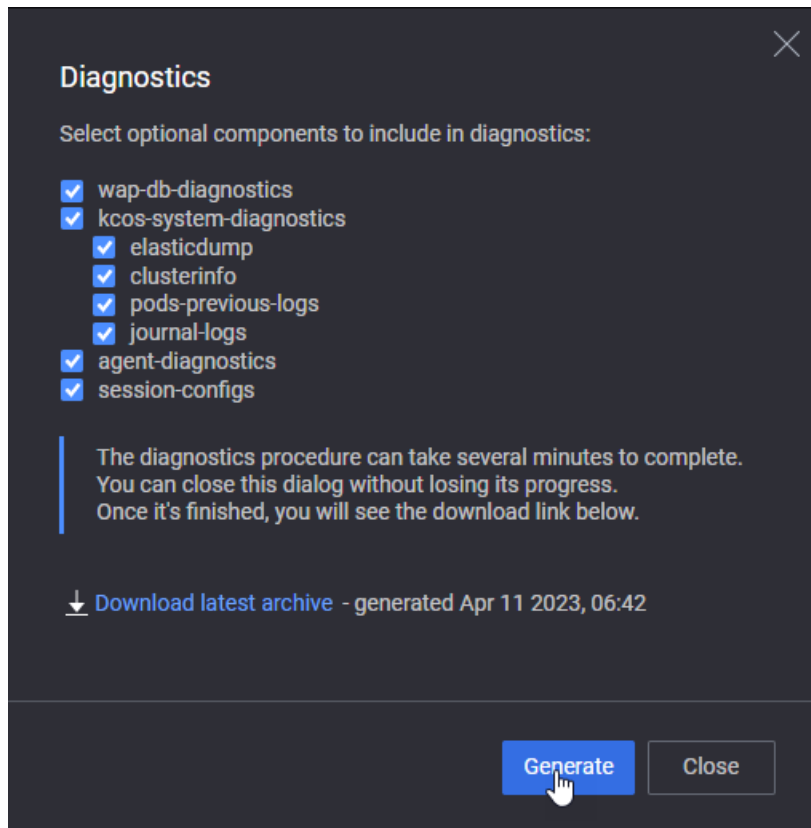
Collect Diagnostics, Cleanup and Data Migration

Collect Diagnostics

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

To collect diagnostics, do the following:

1. Select the Help menu (question mark icon)> **Collect Diagnostics**. The Diagnostics window appears.



2. If needed, select the optional components to include in the diagnostics report.
3. Select **Generate**. The diagnostics procedure can take several minutes to complete. Once it is finished, a download link will be displayed.
4. Select the download link in order to retrieve the diagnostics report.

Collect Logs

To collect logs info, do the following:

1. Click on **Logs Level** in the **Settings** menu. The Controller Logs Level window appears.
2. 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 in order to retrieve the diagnostics report.

System Monitor

CoreSIM system monitor tool is used to check the controller health and review the used resources and their availability. Also, it allows to perform a system cleanup:

1. Click on **System Monitor** in the **Settings** menu.
2. Select the required option:
 - **Controller Health** - this will open the Controller Health dashboard, where the available controller resources are displayed.
 - **System Cleanup** - this will open the System Cleanup window where the size of the following items are displayed: **Logs size**, **Diagnostics size**, **Migration size**. Use the **Delete** button to delete the archives.

Data Migration

CoreSIM data migration tool allows you to migrate controller data from one setup to another. You can export authentication data and other data (such as configurations, external license servers, controller proxies, and results) from a source controller, which you can then import to a new target controller. When the import procedure is complete, the resources that you imported from the source controller will have replaced all the existing data on the target controller.

IMPORTANT The export procedure cannot run when the available controller disk space is lower than 50%. To free up disk space by removing diagnostics, logs, or migration archives, use the **System cleanup** option under the **Settings** menu > **System Monitor**.

To export data from the source controller:

1. From the **Settings** menu, select **Data Migration > Export Controller**. The **Export Controller Data** window opens informing you of the components to be exported.
2. Click the **Start** button. A notification at the bottom of the screen informs you that the migration package is being queued in preparation for export, and the **Export Controller Data** will automatically close.

When all the export resources are collected and available on your local system, a notification informs you that the export package was created.

The export package is downloaded on your local system in the form of a compressed .zip file, under your usual downloads location (for example, *C:\Users\<user name>\Downloads\migrate_package1676028828*)

To import data on the target controller:

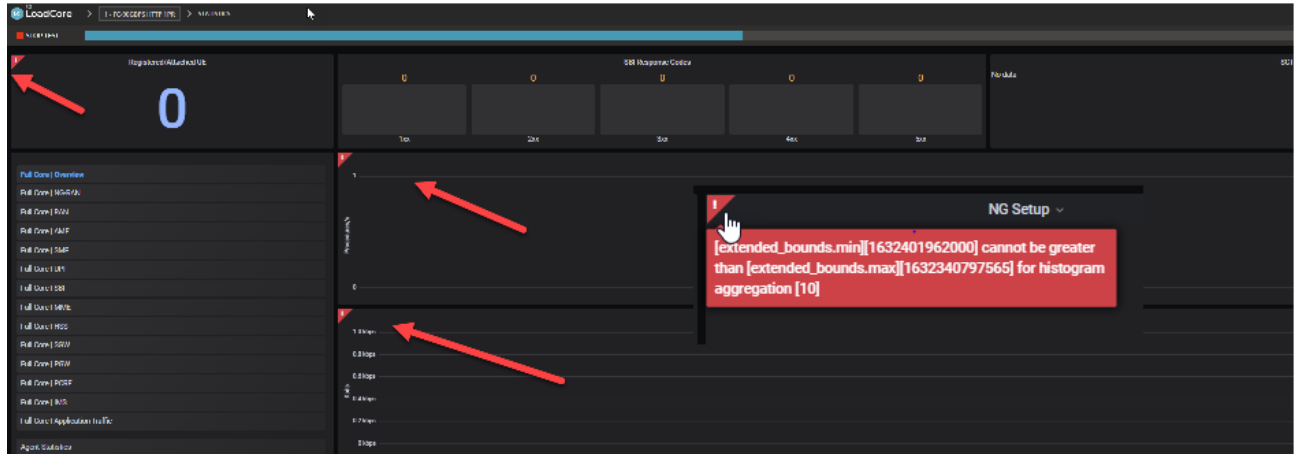
1. From the **Settings** menu, select **Data Migration > Import Controller**. The **Import Controller Data** window opens.
2. Click **Select migrate package for upload**, and select the migration package that you exported from the source controller, and click **Open**.
A warning is displayed informing you that the import procedure cannot be canceled or reverted after it is initiated.
3. Confirm acknowledgment of data loss by selecting the **I understand this will wipe existing data** check box.
4. Click the **Start** button.

The import procedure initiates. The application screen is grayed out during import and will become active again when the import procedure is complete.

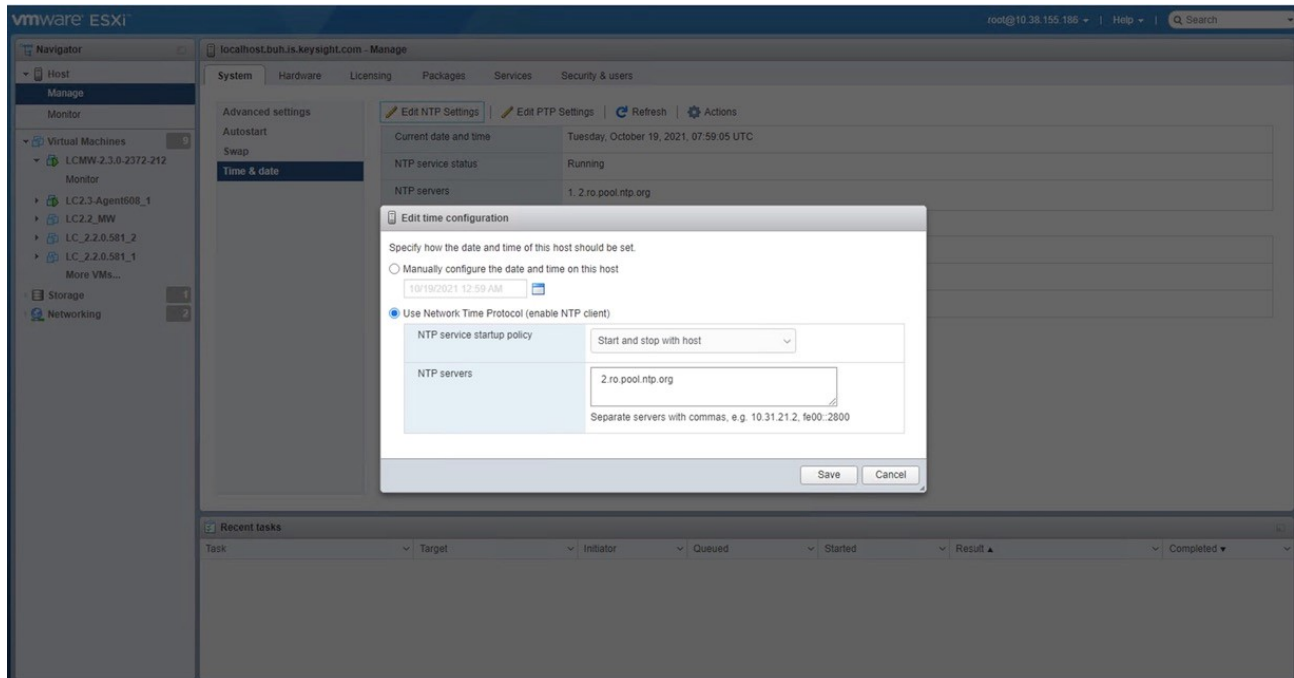
5. After the import procedure is finished, close the **Import Controller Data** window.
6. Log out of the web UI, and log in again to see the newly imported controller data.

NTP troubleshooting

If you are experiencing issues with UI statistics appearing delayed or not showing at all, the cause might be related to NTP.



If you are using ESX make sure the NTP server is set:



To check if the time is in sync on the middleware and agents, you can run the following commands:

- on agents:
`date`
`ntpq -p`
`sudo systemctl status ntp`
- on middleware:
`date`
`kcos date-time time-zone show`
`kcos date-time ntp-servers show`

You can also try to disable and enable NTP settings on the middleware:

```
kcos date-time ntp disable
```

```
kcos date-time ntp enable
```

The default NTP for CoreSim Middleware is `ntp.ubuntu.com`. If you are using a local or another NTP server it is best to change it with:

```
kcos date-time ntp-servers set (it should also be the same as the one set in ESX)
```

IMPORTANT

Start the NTP service on the agents (usually done when `agent-setup.sh` is run) only after setting the clock/NTP server on the middleware. Setting the clock on the middleware after the `btppservice` started on the agents can lead to it panicking (agent side) on big adjustments on sync. Restarting `ntp` agent side (`sudo systemctl restart ntp`) should fix this.

This page intentionally left blank.

APPENDIX A

Predefined Applications

The following table describes the available Predefined Applications.

Application	Description
Adobe Reader Updates Chrome	This application simulates Adobe Reader Updates web application with the Google Chrome browser.
Adobe Reader Updates Firefox	This application simulates Adobe Reader Updates web application with the Google Firefox browser.
Adobe Reader Updates Internet Explorer	This application simulates Adobe Reader Updates web application with the Google Internet Explorer browser.
Adobe Reader Updates Microsoft Edge	This application simulates Adobe Reader Updates web application with the Google Microsoft Edge browser.
ADP Chrome	This application simulates ADP web application with the Chrome browser.
ADP Firefox	This application simulates ADP web application with the Firefox browser.
ADP Internet Explorer	This application simulates ADP web application with the Internet Explorer browser.
ADP Microsoft Edge	This application simulates ADP web application with the Microsoft Edge browser.
Airbnb Chrome	This application simulates Airbnb web application with the Google Chrome browser.
Airbnb Firefox	This application simulates Airbnb web application with the Mozilla Firefox browser.
Airbnb Internet Explorer	This application simulates Airbnb web application with the Internet Explorer browser.
Airbnb Microsoft Edge	This application simulates Airbnb web application with the Microsoft Edge browser.
appointy Chrome	This application simulates appointy web application with the Chrome browser.
appointy Firefox	This application simulates appointy web application with the Firefox browser.
appointy Internet Explorer	This application simulates appointy web application with the Internet Explorer browser.
appointy Microsoft	This application simulates appointy web application with the Microsoft Edge

Application	Description
Edge	browser.
AWS Console Chrome	This application simulates AWS Console web application with the Chrome browser.
AWS Console Firefox	This application simulates AWS Console web application with the Firefox browser.
AWS Console Internet Explorer	This application simulates AWS Console web application with the Internet Explorer browser.
AWS Console Microsoft Edge	This application simulates AWS Console web application with the Microsoft Edge browser.
AWS S3 Chrome	This application simulates AWS S3 web application with the Google Chrome browser.
AWS S3 Firefox	This application simulates AWS S3 web application with the Mozilla Firefox browser.
AWS S3 Internet Explorer	This application simulates AWS S3 web application with the Internet Explorer browser.
AWS S3 Microsoft Edge	This application simulates AWS S3 web application with the Microsoft Edge browser.
Baidu Chrome	This application simulates Baidu web application with the Chrome browser.
Baidu Firefox	This application simulates Baidu web application with the Firefox browser.
Baidu Internet Explorer	This application simulates Baidu web application with the Internet Explorer browser.
Baidu Maps Chrome	This application simulates Baidu Maps web application with the Google Chrome browser.
Baidu Maps Firefox	This application simulates Baidu Maps web application with the Mozilla Firefox browser.
Baidu Maps Internet Explorer	This application simulates Baidu Maps web application with the Internet Explorer browser.
Baidu Maps Microsoft Edge	This application simulates Baidu Maps web application with the Microsoft Edge browser.
Baidu Microsoft Edge	This application simulates Baidu web application with the Microsoft Edge browser.
Bilibili Chrome	This application simulates Bilibili web application with the Google Chrome browser.

Application	Description
Bilibili Firefox	This application simulates Bilibili web application with the Mozilla Firefox browser.
Bilibili Internet Explorer	This application simulates Bilibili web application with the Internet Explorer browser.
Bilibili Microsoft Edge	This application simulates Bilibili web application with the Microsoft Edge browser.
Cisco Spark Chrome	This application simulates Cisco Spark web application with the Chrome browser.
Cisco Spark Firefox	This application simulates Cisco Spark web application with the Firefox browser.
Cisco Spark Internet Explorer	This application simulates Cisco Spark web application with the Internet Explorer browser.
Cisco Spark Microsoft Edge	This application simulates Cisco Spark web application with the Microsoft Edge browser.
Commvault Chrome	This application simulates Commvault web application with the Google Chrome browser.
Commvault Firefox	This application simulates Commvault web application with the Mozilla Firefox browser.
Commvault Internet Explorer	This application simulates Commvault web application with the Internet Explorer browser.
Commvault Microsoft Edge	This application simulates Commvault web application with the Microsoft Edge browser.
Crawling Wikipedia (Chinese) Chrome	This application simulates Crawling Wikipedia (Chinese) web application with the Chrome browser.
Crawling Wikipedia (Chinese) Firefox	This application simulates Crawling Wikipedia (Chinese) web application with the Firefox browser.
Crawling Wikipedia (Chinese) Internet Explorer	This application simulates Crawling Wikipedia (Chinese) web application with the Internet Explorer browser.
Crawling Wikipedia (Chinese) Microsoft Edge	This application simulates Crawling Wikipedia (Chinese) web application with the Microsoft Edge browser.

Application	Description
DocuSign Chrome	This application simulates DocuSign web application with the Google Chrome browser.
DocuSign Firefox	This application simulates DocuSign web application with the Mozilla Firefox browser.
DocuSign Internet Explorer	This application simulates DocuSign web application with the Internet Explorer browser.
DocuSign Microsoft Edge	This application simulates DocuSign web application with the Microsoft Edge browser.
Dreambox Chrome	This application simulates Dreambox web application with the Google Chrome browser.
Dreambox Firefox	This application simulates Dreambox web application with the Mozilla Firefox browser.
Dreambox Internet Explorer	This application simulates Dreambox web application with the Internet Explorer browser.
Dreambox Microsoft Edge	This application simulates Dreambox web application with the Microsoft Edge browser.
eBanking Chrome to Apache	This application simulates a banking web application with the Google Chrome browser connecting to an Apache web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Firefox to IIS	This application simulates a banking web application with the Mozilla Firefox browser connecting to an IIS web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Internet Explorer to Nginx	This application simulates a banking web application with the Internet Explorer browser connecting to an Nginx web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Microsoft Edge to Apache	This application simulates a banking web application with the Microsoft Edge browser connecting to an Apache web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
EpixNow Chrome	This application simulates EpixNow web application with the Google Chrome browser.
EpixNow Firefox	This application simulates EpixNow web application with the Mozilla Firefox browser.

Application	Description
EpixNow Internet Explorer	This application simulates EpixNow web application with the Internet Explorer browser.
EpixNow Microsoft Edge	This application simulates EpixNow web application with the Microsoft Edge browser.
eShop Chrome to Apache	This application simulates an online shop web application with the Google Chrome browser connecting to an Apache web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Firefox to IIS	This application simulates an online shop web application with the Mozilla Firefox browser connecting to an IIS web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Internet Explorer to Nginx	This application simulates an online shop web application with the Internet Explorer browser connecting to an Nginx web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Microsoft Edge to Apache	This application simulates an online shop web application with the Microsoft Edge browser connecting to an Apache web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
Facebook Audio Chrome	This application simulates Facebook Audio web application with the Google Chrome browser.
Facebook Audio Firefox	This application simulates Facebook Audio web application with the Mozilla Firefox browser.
Facebook Audio Internet Explorer	This application simulates Facebook Audio web application with the Internet Explorer browser.
Facebook Audio Microsoft Edge	This application simulates Facebook Audio web application with the Microsoft Edge browser.
Facebook Chrome	This application simulates Facebook web application with the Google Chrome browser.
Facebook Firefox	This application simulates Facebook web application with the Mozilla Firefox browser.
Facebook Internet Explorer	This application simulates Facebook web application with the Internet Explorer browser.
Facebook Microsoft Edge	This application simulates Facebook web application with the Microsoft Edge browser.

Application	Description
FacebookLive Chrome	This application simulates FacebookLive web application with the Google Chrome browser.
FacebookLive Firefox	This application simulates FacebookLive web application with the Mozilla Firefox browser.
FacebookLive Internet Explorer	This application simulates FacebookLive web application with the Internet Explorer browser.
FacebookLive Microsoft Edge	This application simulates FacebookLive web application with the Microsoft Edge browser.
Gab Chrome	This application simulates Gab web application with the Google Chrome browser.
Gab Firefox	This application simulates Gab web application with the Mozilla Firefox browser.
Gab Internet Explorer	This application simulates Gab web application with the Internet Explorer browser.
Gab Microsoft Edge	This application simulates Gab web application with the Microsoft Edge browser.
Gaode Maps Chrome	This application simulates Gaode Maps web application with the Google Chrome browser.
Gaode Maps Firefox	This application simulates Gaode Maps web application with the Mozilla Firefox browser.
Gaode Maps Internet Explorer	This application simulates Gaode Maps web application with the Internet Explorer browser.
Gaode Maps Microsoft Edge	This application simulates Gaode Maps web application with the Microsoft Edge browser.
Google Classroom Chrome	This application simulates Google Classroom web application with the Chrome browser.
Google Classroom Firefox	This application simulates Google Classroom web application with the Firefox browser.
Google Classroom Internet Explorer	This application simulates Google Classroom web application with the Internet Explorer browser.
Google Classroom Microsoft Edge	This application simulates Google Classroom web application with the Microsoft Edge browser.
Google Drive Chrome	This application simulates Google Drive web application with the Google Chrome browser.

Application	Description
Google Drive Firefox	This application simulates Google Drive web application with the Mozilla Firefox browser.
Google Drive Internet Explorer	This application simulates Google Drive web application with the Internet Explorer browser.
Google Drive Microsoft Edge	This application simulates Google Drive web application with the Microsoft Edge browser.
Google Sheets Chrome	This application simulates Google Sheets web application with the Chrome browser.
Google Sheets Firefox	This application simulates Google Sheets web application with the Firefox browser.
Google Sheets Internet Explorer	This application simulates Google Sheets web application with the Internet Explorer browser.
Google Sheets Microsoft Edge	This application simulates Google Sheets web application with the Microsoft Edge browser.
Google Slides Chrome	This application simulates Google Slides web application with the Chrome browser.
Google Slides Firefox	This application simulates Google Slides web application with the Firefox browser.
Google Slides Internet Explorer	This application simulates Google Slides web application with the Internet Explorer browser.
Google Slides Microsoft Edge	This application simulates Google Slides web application with the Microsoft Edge browser.
GoogleHangouts Chrome	This application simulates GoogleHangouts web application with the Chrome browser.
GoogleHangouts Firefox	This application simulates GoogleHangouts web application with the Firefox browser.
GoogleHangouts Internet Explorer	This application simulates GoogleHangouts web application with the Internet Explorer browser.
GoogleHangouts Microsoft Edge	This application simulates GoogleHangouts web application with the Microsoft Edge browser.
GooglePhotos Chrome	This application simulates GooglePhotos web application with the Chrome browser.
GooglePhotos Firefox	This application simulates GooglePhotos web application with the Firefox browser.

Application	Description
GooglePhotos Internet Explorer	This application simulates GooglePhotos web application with the Internet Explorer browser.
GooglePhotos Microsoft Edge	This application simulates GooglePhotos web application with the Microsoft Edge browser.
HTTP App	This application simulates a generic HTTP application.
Jingdong Chrome	This application simulates Jingdong web application with the Google Chrome browser.
Jingdong Firefox	This application simulates Jingdong web application with the Mozilla Firefox browser.
Jingdong Internet Explorer	This application simulates Jingdong web application with the Internet Explorer browser.
Jingdong Microsoft Edge	This application simulates Jingdong web application with the Microsoft Edge browser.
Jira Chrome	This application simulates Jira web application with the Chrome browser.
Jira Firefox	This application simulates Jira web application with the Firefox browser.
Jira Internet Explorer	This application simulates Jira web application with the Internet Explorer browser.
Jira Microsoft Edge	This application simulates Jira web application with the Microsoft Edge browser.
League of Legends Chrome	This application simulates League of Legends web application with the Google Chrome browser.
League of Legends Firefox	This application simulates League of Legends web application with the Mozilla Firefox browser.
League of Legends Internet Explorer	This application simulates League of Legends web application with the Internet Explorer browser.
League of Legends Microsoft Edge	This application simulates League of Legends web application with the Microsoft Edge browser.
Mail.ru Chrome	This application simulates Mail.ru web application with the Chrome browser.
Mail.ru Firefox	This application simulates Mail.ru web application with the Firefox browser.
Mail.ru Internet Explorer	This application simulates Mail.ru web application with the Internet Explorer browser.
Mail.ru Microsoft Edge	This application simulates Mail.ru web application with the Microsoft Edge browser.

Application	Description
Meraki Chrome	This application simulates Meraki web application with the Google Chrome browser.
Meraki Firefox	This application simulates Meraki web application with the Mozilla Firefox browser.
Meraki Internet Explorer	This application simulates Meraki web application with the Internet Explorer browser.
Meraki Microsoft Edge	This application simulates Meraki web application with the Microsoft Edge browser.
Mewe Chrome	This application simulates Mewe web application with the Google Chrome browser.
Mewe Firefox	This application simulates Mewe web application with the Mozilla Firefox browser.
Mewe Internet Explorer	This application simulates Mewe web application with the Internet Explorer browser.
Mewe Microsoft Edge	This application simulates Mewe web application with the Microsoft Edge browser.
MongoDB	This application simulates the MongoDB, a cross-platform document-oriented database.
Netease Music Chrome	This application simulates Netease Music web application with the Google Chrome browser.
Netease Music Firefox	This application simulates Netease Music web application with the Mozilla Firefox browser.
Netease Music Internet Explorer	This application simulates Netease Music web application with the Internet Explorer browser.
Netease Music Microsoft Edge	This application simulates Netease Music web application with the Microsoft Edge browser.
Office 365 Outlook People Chrome	This application simulates Office 365 Outlook People web application with the Chrome browser.
Office 365 Outlook People Firefox	This application simulates Office 365 Outlook People web application with the Firefox browser.
Office 365 Outlook People Internet Explorer	This application simulates Office 365 Outlook People web application with the Internet Explorer browser.
Office 365 Outlook	This application simulates Office 365 Outlook People web application with the

Application	Description
People Microsoft Edge	Microsoft Edge browser.
Office365 Excel Chrome	This application simulates Office365 Excel web application with the Google Chrome browser.
Office365 Excel Firefox	This application simulates Office365 Excel web application with the Mozilla Firefox browser.
Office365 Excel Internet Explorer	This application simulates Office365 Excel web application with the Internet Explorer browser.
Office365 Excel Microsoft Edge	This application simulates Office365 Excel web application with the Microsoft Edge browser.
Office365 OneDrive Chrome	This application simulates Office365 OneDrive web application with the Google Chrome browser.
Office365 OneDrive Firefox	This application simulates Office365 OneDrive web application with the Mozilla Firefox browser.
Office365 OneDrive Internet Explorer	This application simulates Office365 OneDrive web application with the Internet Explorer browser.
Office365 OneDrive Microsoft Edge	This application simulates Office365 OneDrive web application with the Microsoft Edge browser.
Office365 Outlook Chrome	This application simulates Office365 Outlook web application with the Google Chrome browser.
Office365 Outlook Firefox	This application simulates Office365 Outlook web application with the Mozilla Firefox browser.
Office365 Outlook Internet Explorer	This application simulates Office365 Outlook web application with the Internet Explorer browser.
Office365 Outlook Microsoft Edge	This application simulates Office365 Outlook web application with the Microsoft Edge browser.
OK.ru Chrome	This application simulates OK.ru web application with the Chrome browser.
OK.ru Firefox	This application simulates OK.ru web application with the Firefox browser.
OK.ru Internet Explorer	This application simulates OK.ru web application with the Internet Explorer browser.
OK.ru Microsoft Edge	This application simulates OK.ru web application with the Microsoft Edge browser.

Application	Description
Portal Chrome to Apache	This application simulates a portal web application with the Google Chrome browser connecting to an Apache web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Firefox to IIS	This application simulates a portal web application with the Mozilla Firefox browser connecting to an IIS web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Internet Explorer to Nginx	This application simulates a portal web application with the Internet Explorer browser connecting to an Nginx web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Microsoft Edge to Apache	This application simulates a portal web application with the Microsoft Edge browser connecting to an Apache web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Reddit Chrome	This application simulates Reddit web application with the Google Chrome browser.
Reddit Firefox	This application simulates Reddit web application with the Mozilla Firefox browser.
Reddit Internet Explorer	This application simulates Reddit web application with the Internet Explorer browser.
Reddit Microsoft Edge	This application simulates Reddit web application with the Microsoft Edge browser.
Salesforce Chrome	This application simulates Salesforce web application with the Chrome browser.
Salesforce Firefox	This application simulates Salesforce web application with the Firefox browser.
Salesforce Internet Explorer	This application simulates Salesforce web application with the Internet Explorer browser.
Salesforce Microsoft Edge	This application simulates Salesforce web application with the Microsoft Edge browser.
Service-Now Chrome	This application simulates Service-Now web application with the Google Chrome browser.
Service-Now Firefox	This application simulates Service-Now web application with the Mozilla Firefox browser.
Service-Now	This application simulates Service-Now web application with the Internet

Application	Description
Internet Explorer	Explorer browser.
Service-Now Microsoft Edge	This application simulates Service-Now web application with the Microsoft Edge browser.
Skype 8 Chrome	This application simulates Skype 8 web application with the Chrome browser.
Skype 8 Firefox	This application simulates Skype 8 web application with the Firefox browser.
Skype 8 Internet Explorer	This application simulates Skype 8 web application with the Internet Explorer browser.
Skype 8 Microsoft Edge	This application simulates Skype 8 web application with the Microsoft Edge browser.
Skype Chrome	This application simulates Skype web application with the Chrome browser.
Skype Firefox	This application simulates Skype web application with the Firefox browser.
Skype Internet Explorer	This application simulates Skype web application with the Internet Explorer browser.
Skype Microsoft Edge	This application simulates Skype web application with the Microsoft Edge browser.
SMTP	Emulates an SMTP Email session.
Social Network Chrome to Apache	This application simulates a social network web application with Google Chrome browser connecting to an Apache web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Firefox to IIS	This application simulates a social network web application with Mozilla Firefox browser connecting to an IIS web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Internet Explorer to Nginx	This application simulates a social network web application with Internet Explorer browser connecting to an Nginx web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Microsoft Edge to Apache	This application simulates a social network web application with Microsoft Edge browser connecting to an Apache web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Splunk Chrome	This application simulates Splunk web application with the Google Chrome browser.

Application	Description
Splunk Firefox	This application simulates Splunk web application with the Mozilla Firefox browser.
Splunk Internet Explorer	This application simulates Splunk web application with the Internet Explorer browser.
Splunk Microsoft Edge	This application simulates Splunk web application with the Microsoft Edge browser.
Tubi Chrome	This application simulates Tubi web application with the Chrome browser.
Tubi Firefox	This application simulates Tubi web application with the Firefox browser.
TWC Firefox	This application simulates TWC web application with the Firefox browser.
TWC Internet Explorer	This application simulates TWC web application with the Internet Explorer browser.
TWC Microsoft Edge	This application simulates TWC web application with the Microsoft Edge browser.
Video Platform Chrome to Apache	This application simulates a video platform web application with Google Chrome browser connecting to an Apache web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Firefox to IIS	This application simulates a video platform web application with Mozilla Firefox browser connecting to an IIS web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Internet Explorer to Nginx	This application simulates a video platform web application with Internet Explorer browser connecting to an Nginx web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Microsoft Edge to Apache	This application simulates a video platform web application with Microsoft Edge browser connecting to an Apache web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Vkontakte Chrome	This application simulates VKontakte web application with the Chrome browser.
Vkontakte Firefox	This application simulates VKontakte web application with the Firefox browser.
Vkontakte Internet Explorer	This application simulates VKontakte web application with the Internet Explorer browser.

Application	Description
Vkontakte Microsoft Edge	This application simulates VKontakte web application with the Microsoft Edge browser.
Yammer Chrome	This application simulates Yammer web application with the Google Chrome browser.
Yammer Firefox	This application simulates Yammer web application with the Mozilla Firefox browser.
Yammer Internet Explorer	This application simulates Yammer web application with the Internet Explorer browser.
Yammer Microsoft Edge	This application simulates Yammer web application with the Microsoft Edge browser.
YYLive Chrome	This application simulates YYLive web application with the Google Chrome browser.
YYLive Firefox	This application simulates YYLive web application with the Mozilla Firefox browser.
YYLive Internet Explorer	This application simulates YYLive web application with the Internet Explorer browser.
YYLive Microsoft Edge	This application simulates YYLive web application with the Microsoft Edge browser.

APPENDIX B

Application Actions

The following table lists the application actions and action parameters available in CoreSIM.

Application Action	Action Parameters	Parameter Description
<i>Adobe Reader Updates</i>		
Check For Updates	Current Version	Displays the current version.
	Update Version	Displays the update version.
Download Updates	Update Version	Displays the current version.
<i>ADP</i>		
Load Main Paige	N/A	N/A
Load Login Information Page	N/A	N/A
Load Employee Login Page	N/A	N/A
<i>Airbnb</i>		
Load First Page	City	Set the city name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
Specify Search Criteria	City	Set the city name.
	State/province	Ste the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Second selected rental	Set the second selected rental name.

Application Action	Action Parameters	Parameter Description
Select a Rental	Main rental photo	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Main rental photo (low resolution)	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo of host	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 2 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 3 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 4 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 5 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
	City	Set the city name.
	State/province	Ste the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Airbnb host name	Set the airbnb host name.
	Reviewer	Set the reviewer name.
	Second reviewer	Set the second reviewer name.
	Third reviewer	Set the third reviewer name.
View Rental Photos	Thumbnail photo of host	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Thumbnail photo of first reviewer	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Thumbnail photo of third reviewer	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	State/province	Ste the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.

Application Action	Action Parameters	Parameter Description
	Checkout Date	Set the check-out date.
View More Amenities	City	Set the city name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
View Hot Profile	Thumbnail photo of first reviewer	
	Photo 3 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	State/province	Ste the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Airbnb host name	Set the airbnb host name.
	Reviewer	Set the reviewer name.
	Second reviewer	Set the second reviewer name.
	Third reviewer	Set the third reviewer name.
	Second selected rental	Set the second selected rental name.
View Second Property	Photo 1 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
	Photo 4 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 5 of rental	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	Second selected rental	Set the second selected rental name.
View the Calendar	N/A	N/A
<i>appointy</i>		
Load Login Page	User name	Set the user name.
Login	User name	Set the user name.
	Password	Provide the password
	Profession	Set the profession.
	City	Set the city name.
	State/Province	Set the state/province name.
	Staff member 1	Set the name of the first staff member.
	Staff member 2	Set the name of the second staff member.
	Customer 1 first name	Set the first name of Customer 1.
	Customer 1 last name	Set the last name of Customer 1.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.

Application Action	Action Parameters	Parameter Description
Book New Customer	User name	Set the user name.
	Full manager name	Set the manager name.
	City	Set the city name.
	State/Province	Set the state/province name.
	Service	Set the service name.
	Staff member 1	Set the name of the first staff member.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.
View New Users Pulldown	User name	Set the user name.
View New Appointments Pulldown	User name	Set the user name.
Select Dashboard Tab	User name	Set the user name.
	Profession	Set the profession.
Select Reports Tab	User name	Set the user name.
View Week Calendar	User name	Set the user name.
View Customers Tab	User name	Set the user name.
	City	Set the city name.
	Customer 1 first name	Set the first name of Customer 1.
	Customer 1 last name	Set the last name of Customer 1.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.

Application Action	Action Parameters	Parameter Description
Logout	User name	Set the user name.
<i>AWS Console</i>		
Load AWS Page	N/A	N/A
Load AWS Management Console	Region name	Set the region name.
Sign In	User email	Provide the user email.
	Password	Provide the password.
	User name	Set the user name.
	Region name	Set the region name.
Check Account Info	User email	Provide the user email.
	Region name	Set the region name.
Check Account Billing	User email	Provide the user email.
	Region name	Set the region name.
Check Credentials	Region name	Set the region name.
	Existing keyID 1	Provide the existing keyID 1.
	Existing keyID 2	Provide the existing keyID 2.
Create New Access Key	New KeyID	Set the new keyID.
Download Key file	New KeyID	Set the new keyID.
	Key file name	Set the key file name.
Delete Key	Existing keyID 1	Provide the existing keyID 1.
Sign Out	User email	Provide the user email.
	Region name	Set the region name.
<i>AWS S3</i>		

Application Action	Action Parameters	Parameter Description
Check Buckets Names	User email	Provide the user email.
	Region name	Set the region name.
	KeyID	Provide the keyID.
Create Buckets	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
Upload File	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Local file name for upload	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
List Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Source file name	Set the source file name.
Copy Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
	Source file name	Set the source file name.

Application Action	Action Parameters	Parameter Description
Verify Copied Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Destination bucket name	Set the destination bucket name.
Download Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Source file name	Set the source file name.
Delete Files and Buckest	User email	Provide the user email.
	Region name	Set the region name.
	KeyID	Provide the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
	Source file name	Set the source file name.
<i>Baidu</i>		
Access Baidu News	N/A	N/A
Access Baidu Maps	N/A	N/A
Access Baidu Pictures	N/A	N/A
Load Maine Paige	N/A	N/A
Search String	Search query	Provide the search criteria.
Search Image	Baidu search image file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
Access Baidu Passport	N/A	N/A
<i>Baidu Maps</i>		
Load Web Page	N/A	N/A
Search a Place	Query string	Provide the search criteria.
Finding a route	Query string	Provide the search criteria.
	Source location	Set the search location.
	Destination location	Set the destination location.
<i>Bilibili</i>		
Open Bilibili Website	N/A	N/A
Login	Username	Provide the username.
	Password	Provide the password.
Search Video	Video name	Provide the video name.
Watch Video	N/A	N/A
Upload Video	Uploaded video title	Set the title for the uploaded video.
	Uploaded video file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout	N/A	N/A
<i>Cisco Spark</i>		
Start the Application	N/A	N/A
Click Get Started	N/A	N/A
Click Next	User email address	Provide the user's email address.
Click SignIn	The contact's	Provide the contact's first/last name.

Application Action	Action Parameters	Parameter Description
	first/last name	
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
	Password	Provide the password.
	User's first/last name	Provide the user's first/last name
Create a Team	User email address	Provide the user's email address.
Add Contact	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Send Message	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Send File	User email address	Provide the user's email address.
	User's first/last name	Provide the user's first/last name
Initiate a Call	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.

Application Action	Action Parameters	Parameter Description
Hang Up Call	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Exit	N/A	N/A
<i>Commvault</i>		
Get Login Page	N/A	N/A
Login	User email	Provide the user's email address.
	Password	Provide the password.
View Drive	N/A	N/A
Create Folder	Created folder name	Set the name of the created folder.
Rename Folder	Folder name	Set the folder's new name.
Move File	Folder name	Provide the folder name.
Navigate To Folder	Folder name	Provide the folder name.
Upload File	Uploaded file name	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Download File	Downloaded file name	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Get Public Link	Folder ID	Provide the folder ID.
Move File To Trash	N/A	N/A
View Trash	N/A	N/A

Application Action	Action Parameters	Parameter Description
Restore File From Trash	Folder name	Provide the folder name.
Empty Trash	N/A	N/A
View Public Links	N/A	N/A
Deelte Public Link	Folder ID	Provide the folder ID.
Log Out	N/A	N/A
<i>Crawling Wikipedia (Chinese)</i>		
Crawl Link 1	Root URI	Set the root URI.
Crawl Link 2	Root URI	Set the root URI.
Crawl Link 3	Root URI	Set the root URI.
Crawl Link 4	Root URI	Set the root URI.
<i>DocuSign</i>		
Load Front Page	N/A	N/A
<i>Dreambox</i>		
Login	Login email address	Provide the login email address.
	Password	Provide the password.
Open Dashboard	N/A	N/A
Check Activity Status	From date	Set the starting date.
	To date	Set the end date.
Add Assignment	Select a grade	Set a grade.
	Select a category	Set a category.
	Short description	provide a short description.
Set Dreambox Game	N/A	N/A
Pause Dreambox Game	N/A	N/A
Quit Dreambox	N/A	N/A

Application Action	Action Parameters	Parameter Description
Game		
Logout	N/A	N/A
<i>eBanking</i>		
Sign Up	SignUp username	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	SignUp password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	SignUp confirm password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Login	Login username	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
View Transactions	N/A	N/A
View Accounts	N/A	N/A
Get Contact Page	N/A	N/A
Logout	N/A	N/A
<i>EpixNow</i>		

Application Action	Action Parameters	Parameter Description
Open Login Page	N/A	N/A
Login	Email	Provide the login email address.
	Password	Provide the password.
Browse Movies	Search keyword	Provide the search criteria.
Search Movies	Search keyword	Provide the search criteria.
Play	Search keyword	Provide the search criteria.
Logout	N/A	N/A
<i>eShop</i>		
Search Product	Product name	Provide the product name.
View Product	Product ID	Provide the product ID.
Login	Login username	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Add To Cart	N/A	N/A
Remove From Cart	N/A	N/A
Buy	Full name	Provide the full name.
	Address	Provide the address.
	Account number	Provide the account number.
Logout	N/A	N/A
<i>Facebook Audio</i>		
Open Home Page	N/A	N/A
Login	Encrypted	Provide the password.

Application Action	Action Parameters	Parameter Description
	password	
	Email	Provide the login email address.
Create Audio Room	N/A	N/A
Join Audio Room	N/A	N/A
Leave Audio Room	N/A	N/A
Logout	N/A	N/A
<i>Facebook</i>		
Get Homepage	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User first name	Provide the first name.
	User second name	Provide the second name.
Open Notifications	N/A	N/A
Search Person	Search string	Provide the search criteria.
Add Friend	Friend first name	Provide the friend's first name.
	Friend second name	Provide the friend's second name.
Send Message	Message body	Provide the message.
	Recipient first name	Provide the recipient's first name.
	Recipient second name	Provide the recipient's second name.

Application Action	Action Parameters	Parameter Description
Send Message With Attachment	Message body	Provide the message.
	Recipient first name	Provide the recipient's first name.
	Recipient second name	Provide the recipient's second name.
	Filename	Provide the file name
	Upload File	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Download Attachment	Download file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Go To Profile	N/A	N/A
Post In News Feed	Post Message	Provide the message.
	Post file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Comment Post	Comment message	Provide the post message.
	Post author	Provide the post's author.
Delete Comment	Post author	Provide the post's author.
Like Post	N/A	N/A
Unlike Post	N/A	N/A
Sign Out	N/A	N/A
<i>FacebookLive</i>		

Application Action	Action Parameters	Parameter Description
Sign In	C_user cookie2	Set the value.
	C_user cookie	Set the value.
	User email address	Provide the user email address.
	Password	Provide the password.
	User name	Provide the username.
	Friend 1 first name	Provide the first name.
Start Live Stream	C_user cookie	Set the value.
	User name	Provide the username.
	Friend 1 first name	Provide the first name.
	Friend 3 first name	Provide the first name.
	Video stream ID	Set the video stream ID.
Sign Out	C_user cookie	Set the value.
	User email address	Provide the user email address.
	User name	Provide the username.
	Video stream ID	Set the video stream ID.
<i>Gab</i>		
Open Home Page	N/A	N/A
Open Login Page	N/A	N/A
Login	Email	Provide the email address.
	Password	Provide the password.
Read News	N/A	N/A
Post News	Statut text	Provide the message.
Logout	N/A	N/A

Application Action	Action Parameters	Parameter Description
<i>Gaode Maps</i>		
Open Website	N/A	N/A
Search Location	Destination	Provide the destination.
Find Route	Destination	Provide the destination.
	Starting location	Provide the starting location.
	Transportation method	Provide the transportation method.
<i>Google Classroom</i>		
Load Homepage	N/A	N/A
Login	Username	Provide the username.
	User email	Provide the email address.
	User password	Provide the password.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
Create New Classroom	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Create New Post	Post text	Provide the text message.
Edit Post	Post text	Provide the text message.
Add Attachment to Post	Post attachment	Select an option:

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Post text	Provide the text message.
Load Classroom Tab	N/A	N/A
Create New Assignment	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Add Attachment to Assignment	Assignment document	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Assignment title	Provide the assignment title.
Load People Tab	N/A	N/A
Invite a Student	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.

Application Action	Action Parameters	Parameter Description
Student Load Homepage	Post attachment	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Student Add Submission	Submission document compressed	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Add Student Private Comment	Student private comment	Provide the comment.
Load Grades Tab	Assignment title	Provide the assignment title.

Application Action	Action Parameters	Parameter Description
View Submission	Submission document	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Submission document webp format	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Assignment title	Provide the assignment title.
	Student private comment	Provide the comment.
Add Professor Private Comment	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Assignment title	Provide the assignment title.
	Student private comment	Provide the comment.
	Professor private comment	Provide the comment.
Grade Submission	Grade of the	Provide the grade value.

Application Action	Action Parameters	Parameter Description
	assignment	
Archive Classroom	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Delete Classroom	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Logout	Username	Provide the username.
	User email	Provide the email address.
<i>Google Drive</i>		
Get Sign In Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Create Folder	Folder name	Set the folder name.
Upload File	File name	Provide the file name.
	Upload file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value.

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Delete File	File name	Provide the file name.
Empty Bin	File name	Provide the file name.
	File content	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Create Text Document	Document content	Provide the document content.
	Document name	Provide the document name.
Create Presentation	Powerpoint content	Provide the content.
	Powerpoint name	Provide the name.
Create Spreadsheet	Spreadsheet content	Provide the content.
	Spreadsheet name	Provide the name.
Download File	File name	Provide the file name.
	Downloaded file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Sign Out	N/A	N/A
<i>Google Sheets</i>		
Load Sign In Page	N/A	N/A
Sign In	Username	Provide the username.
	Password	Provide the password.

Application Action	Action Parameters	Parameter Description
Create a New Sheet	N/A	N/A
Input Data	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Key text 1	Provide the key text.
	Value text 1	Provide the value text
	Key text 2	Provide the key text.
	Value text 2	Provide the value text
	Key text 3	Provide the key text.
	Value text 3	Provide the value text
Share the Sheet	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Receiver username	Provide the username of the reciever.
Complete sharing	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Receiver username	Provide the username of the receiver.
	Sharing note	Provide the text for the sharing note.
Sign Out	Username	Provide the username.
<i>Google Slides</i>		
Load Sigh In Page	N/A	N/A
Sign In	Username	Provide the username.
	Password	Provide the password.
Start a New Presentation	Username	Provide the username.
Start a New Slide	N/A	N/A
Input Slide Text	Slide Name	Provide the value.

Application Action	Action Parameters	Parameter Description
Replace Image	Username	Provide the username.
	File attachment	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Name the Slide	Slide name	Provide the value.
Share the Slide	Username	Provide the username.
	Slide name	Provide the value.
	Receiver username	Provide the username of the receiver.
Send Sharing	Receiver username	Provide the username of the receiver.
Sign Out	Username	Provide the username.
<i>GoogleHangouts</i>		
Load First Page	N/A	N/A
Sign In	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Password	Provide the password.
	Other user's first/last name	Provide the other user's first/last name.
Start Chat	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
Send Text Message	First chat text message	Provide the text message.

Application Action	Action Parameters	Parameter Description
Receive Text Message	N/A	N/A
Send a File	User email address	Provide the user email address.
	Second chat text message	Provide the text message.
Receive Text Reply	User email address	Provide the user email address.
Send Image	N/A	N/A
Receive Image	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
	First chat text message	Provide the text message.
	Second chat text message	Provide the text message.
Make Phone Call	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Phone number	Provide the phone number.
Start Video Call	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
Logout	User's first/last name	Provide the user's first/last name.

Application Action	Action Parameters	Parameter Description
	User email address	Provide the user email address.
<i>GooglePhotos</i>		
Load Login Page	N/A	N/A
Login to Google	Password	Provide the password.
	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
View a Photo	User email address	Provide the user email address.
	Full user name	Provide the username.
View Next Photo	Full user name	Provide the username.
Return to Main Page	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
View Albums Page	Shared folder name	Provide the folder name.
Select an Album	User email address	Provide the user email address.
	Full user name	Provide the username.
	Shared folder name	Provide the folder name.
Upload a Photo	Uploaded Photo	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to

Application Action	Action Parameters	Parameter Description
		upload a file.
Return to Photos Page	N/A	N/A
Download a Photo	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout of Google	User email address	Provide the user email address.
	Full user name	Provide the username.
<i>HTTP</i>		

Application Action	Action Parameters	Parameter Description
HTTP GET	Path	The value of the path requested.
	Query	The value of the query requested.
	Request headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Accept-Language • Sec-Fetch-User • Upgrade-Insecure-Requests • Sec-Fetch-Site <p>Use the Add button to add new options or the Delete to remove them.</p>
	Status code	The value of the response status code.
	Reason phrase	The value of the reason phrase.
	Response headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Cache-Control • Etag <p>Use the Add button to add new options or the Delete to remove them.</p>
	Response body	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file. • Dynamic payload - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
HTTP POST	URL	Provide the URL.
	Request headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Sec-Fetch-User • Upgrade-Insecure-Requests • Accept-Language • Sec-Fetch-Site <p>Use the Add button to add new options or the Delete to remove them.</p>
	Request body	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file. • Dynamic payload - select an option from the drop-down list or use the Upload button to upload a file.
	Status code	The value of the response status code.
	Reason phrase	The value of the reason phrase.
	Response headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Etag • Cache-Control <p>Use the Add button to add new options or the Delete to remove them.</p>
	Response Body	Add a response message.
<i>Jingdong</i>		
Go To Jingdong	N/A	N/A
Login	Username	Provide the username.
Search For products	Search keyword	Provide the search criteria.
Check Products Information	N/A	N/A

Application Action	Action Parameters	Parameter Description
Checkout	Username	Provide the username.
	Product name	Provide the product name.
	Order ID	Provide the order ID.
Logout	N/A	N/A
<i>Jira</i>		
Load Login Page	Story name	Provide the story name.
Login	Login email address	Provide the login email address.
	Password	Provide the password.
Create Project	Login email address	Provide the login email address.
	Project name	Provide the project name.
Create Story	Project name	Provide the project name.
	Story name	Provide the story name.
Add Comments to Story	Story name	Provide the story name.
Mark The Story To Closed	Story name	Provide the story name.
Logout	Story name	Provide the story name.
<i>League of Legends</i>		
Login	User ID	Provide the user ID.
Start Game	User ID	Provide the user ID.
Attack	N/A	N/A
<i>Mail.ru</i>		
Login	Username	Provide the username.
	Password	Provide the password.

Application Action	Action Parameters	Parameter Description
Send Mail	Fullname	Provide the fullname.
	Recipient email address	Provide the recipient email address.
	Recipient email subject	Provide the email subject.
	Recipient email body	Provide the email body.
View Mail	Fullname	Provide the fullname.
	Message sender email	Provide the sender email.
	Message sender name	Provide the sender name.
	View message subject	Provide the message subject.
	View message body	Provide the message body.
Logout	N/A	N/A
<i>Meraki</i>		
Login	Dashboard email address	Provide the email address.
	Dashboard password	Provide the password.
Enroll Device	New device address	Provide the device address.
	Enrollment message	Provide an enrollment message.
Add Application	New device address	Provide the device address.
	New application search query	Provide the search criteria.
Add Profile	New device address	Provide the device address.

Application Action	Action Parameters	Parameter Description
	Test profile name	Provide the test profile name.
	Test profile description	Provide the test profile description.
	Backup file name	Provide the backup file name.
Push Updates	N/A	N/A
View Clients	New device address	Provide the device address.
View Map	New device address	Provide the device address.
View Logs	New device address	Provide the device address.
Download CSV	Dashboard email address	Provide the email address.
Send Command	Remote command line	Provide the remote command line,
View Summary	New device address	Provide the device address.
Add Geofence	Geofence name	Provide the geofence name.
	Area name	Provide the area name.
Add Policy	Policy name	Provide the policy name
Add owner	New device address	Provide the device address.
	Owner name	Provide the name.
	Owner username	Provide the username.
	Owner password	Provide the password.
	Owner email	Provide the email.
Logout	N/A	N/A
<i>Mewe</i>		
Open Login Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Login	Email	Provide the email address.
	Password	Provide the password.
Read News Feed	N/A	N/A
Post Status	Status message	Provide the message text.
Logout	N/A	N/A
<i>MongoDB</i>		
Insert	N/A	N/A
Update	N/A	N/A
Query	N/A	N/A
Get More	N/A	N/A
Delete	N/A	N/A
Kill Cursor	N/A	N/A
Diagnostic Messages	N/A	N/A
<i>Netease</i>		
Go to Netease Music	N/A	N/A
Login	N/A	N/A
Search Music	Artist ID	Provide the artist ID.
PlayMusic	Music file name 1	Provide the music file name.
	Music file name 2	Provide the music file name.
	Music file name 3	Provide the music file name.
	Music file name 4	Provide the music file name.
Add To Playlist	Artist ID	Provide the artist ID.
Recommend Music	Artist ID	Provide the artist ID.

Application Action	Action Parameters	Parameter Description
Watch Music Video	Artist ID	Provide the artist ID.
	Music video ID 1	Provide the music video ID.
	Music video ID 2	Provide the music video ID.
	Music video ID 3	Provide the music video ID.
	Music video ID 4	Provide the music video ID.
Logout	N/A	N/A
<i>Office 365 Outlook People</i>		
Get Sign In Page	N/A	N/A
Sign In	User name	Provide the user name.
	Password	Provide the password.
Create a New Contact	Contact first name	Provide the first name.
	Contact last name	Provide the last name.
	Contact email	Provide the email address.
Search for a Contact	Search people	Provide the search criteria.
Delete a Contact	Contact email	Provide the email address.
Sign Out	N/A	N/A
<i>Office365 Excel</i>		
Get Home Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
Get Excel Tab	N/A	N/A
Get Excel Workbook	Workbook name	Provide the workbook name.
Edit Workbook	Content	Provide the content.
Pin Workbook	Workbook name	Provide the workbook name.
Open Workbook In OneDrive	N/A	N/A
Sign Out	N/A	N/A
<i>Office365 OneDrive</i>		
Get Home Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Get OneDrive Tab	N/A	N/A
Delete File	File name	Provide the file name.
Upload File	File name	Provide the file name.
	Upload file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Create Folder	Folder name	Provide the folder name.
Create Excel Workbook	Workbook name	Provide the workbook name.
Create Word	Document name	Provide the document name.

Application Action	Action Parameters	Parameter Description
Document		
Create Powerpoint Presentation	Powerpoint name	Provide the powerpoint name.
Sign Out	N/A	N/A
<i>Office365 Outlook</i>		
Sign In	User email	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
View Inbox	N/A	N/A
Send Message	Recipient	Provide the email address.
	Subject	Provide the email subject.
	Body	Provide the email body text.
Send Message With Attachment	Recipient	Provide the email address.
	Subject	Provide the email subject.
	Body	Provide the email body text.
	Attachment	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Attachment filename	Provide the file name.
Open Message	N/A	N/A
Delete Message	N/A	N/A

Application Action	Action Parameters	Parameter Description
Navigate To Calendar Panel	N/A	N/A
Create A New Event	Event date	Set the event date.
	Event start time	Set the start time.
	Event end time	Set the end time
	Event name	Set the event name.
Delete An Event	Event date	Set the event date.
	Event start time	Set the start time.
	Event end time	Set the end time
	Event name	Set the event name.
Navigate to People Panel	N/A	N/A
Create a New Contact	Contact email	Provide the address email.
	First name	Provide the first name.
	Second name	Provide the second name.
	Phone number	Provide the phone number.
Search For A Contact	Search string	Provide the search criteria.
Delete A Contact	Contact email	Provide the address email.
	First name	Provide the first name.
	Second name	Provide the second name.
	Phone number	Provide the phone number.
Navigate To Task Panel	N/A	N/A
Create New Task	Task title	Provide the task tile.
Mark Task Completed	Task title	Provide the task tile.
Delete Task	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign Out	N/A	N/A
<i>OK.ru</i>		
Login	Username	Provide the user name.
	Password	Provide the password.
View Feed	N/A	N/A
Post Message	Message	Provide the message text.
Logout	N/A	N/A
<i>Portal</i>		
Login	User email	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Search Image	Search query	Provide the search criteria.
Upload Image	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout	N/A	N/A
<i>Reddit</i>		
Load Main Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign In	Username	Provide the user name.
	Account password	Provide the password.
Access Post	N/A	N/A
Create Comment	Comment content	Provide content for the comment.
Delete Comment	N/A	N/A
Search Posts	Query string	Provide the search criteria.
Subscribe to Subreddit	Subreddit	Provide the subreddit.
Access Gifts Page	Subreddit	Provide the subreddit.
Load Profile	Username	Provide the user name.
Access Settings	N/A	N/A
Access Messages	N/A	N/A
Sign Out	N/A	N/A
<i>Salesforce</i>		
Load Login Page	User name	Provide the user name.
Login	User name	Provide the user name.
	Login email address	Provide the login email address.
	Password	Provide the password.
Select Top Deal	User name	Provide the user name.
	Login email address	Provide the login email address.
Update Call Log	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Opportunities Tab	Login email address	Provide the login email address.

Application Action	Action Parameters	Parameter Description
Select An Opportunity	User name	Provide the user name.
	Login email address	Provide the login email address.
Edit Amount	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Notes Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Edit a Note	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Dashboards Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Opoen Adoption Dashboard	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Calendar Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Add a Meeting	User name	Provide the user name.
	Login email address	Provide the login email address.
Logout	User name	Provide the user name.
	Login email address	Provide the login email address.
<i>Service-Now</i>		
Get Sign In Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign In	Username	Provide the user name.
	Password	Provide the password.
View an Incident	Username	Provide the user name.
	Incident number searched	Provide the incident number.
	Search shot description	Provide a description.
Create an Incident	Username	Provide the user name.
	Incident number searched	Provide the incident number.
	Description	Provide a description.
	Caller	Provide the caller.
	Caller email	Provide the caller email.
Sign Out	N/A	N/A
<i>Skype 8</i>		
Sign In	Sign-in address	Provide the email address.
	Password	Provide the password.
Add Contact	Contact email address	Provide the email address.
	Contact's first/last name	Provide the first/last name.
View Contact Profile	Contact email address	Provide the email address.
Send an IM	N/A	N/A
Receive an IM	N/A	N/A
Start Audio Call	N/A	N/A
End Audio Call	N/A	N/A
Sign Out	N/A	N/A

Application Action	Action Parameters	Parameter Description
<i>Skype</i>		
Login	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
	Peer activity message	Provide the message.
Video Call	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
End Video Call	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
Voice Call	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
End Voice Call	Login email address	Provide the email address.
	User name	Provide the user name.

Application Action	Action Parameters	Parameter Description
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
Logout	Login email address	Provide the email address.
	User name	Provide the user name.
	Peer email address	Provide the peer email address.
	Peer user name	Provide the peer user name.
	Peer activity message	Provide the message.
<i>SMTP</i>		
Ehlo	N/A	N/A
Auth Login	N/A	N/A
Send Mail	Email subject	Provide the email subject.
	Email content	Provide the email content.
	Number of attachment	Provide the value for the number of attachment.
	Attachment Content	Provide the attachment content.
Quit	N/A	N/A
<i>Social Network</i>		
Login	Login username	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a

Application Action	Action Parameters	Parameter Description
		file.
News feed	N/A	N/A
View Profile	Member ID	Provide the member ID.
Like Post	N/A	N/A
Unlike Post	N/A	N/A
Create Post	Post content	Provide the content.
Comment To Post	Original post ID	Provide the post ID.
	Comment content	Provide the content.
Logout	N/A	N/A
<i>Splunk</i>		
Load Login Page	N/A	N/A
Login	Username	Provide the user name.
	Password	Provide the password.
Upload Log	Description	Provide a description.
	Index	Provide the index.
	Log File	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Search Log	Index	Provide the index.
Logout	Username	Provide the user name.
<i>Tubi</i>		
Open Tubi Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Login	Email address	Provide the email address.
	Password	Provide the password.
	User ID	Provide the user ID.
	User name	Provide the user name.
Browse Tubi	Genre	Provide the genre.
Select Movie	Genre	Provide the genre.
	Movie name	Provide the movie name.
	Movie duration	Provide the movie duration.
	Movie description	Provide the movie description.
	Movie director	Provide the movie director.
	Movie release year	Provide the release year.
	Movie actor 1	Provide the movie actor.
	Movie actor 2	Provide the movie actor.
	Movie content ID	Provide the movie content ID.
	Recommended movie name	Provide the recommended movie name.
Play Video	Movie content ID	Provide the movie content ID.
Pause Video	Movie content ID	Provide the movie content ID.
Selet Recommended Movie	Genre	Provide the genre.
	Recommended movie name	Provide the recommended movie name.
	Recommended movie duration	Provide the recommended movie duration.
Logout	N/A	N/A
<i>TWC</i>		
Open The Weather Channel App	N/A	N/A

Application Action	Action Parameters	Parameter Description
View 48 Hours Details	N/A	N/A
View 15 Days Details	N/A	N/A
Swipe to Bottom of Main Page	N/A	N/A
<i>Video Platform</i>		
Login	Login username	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none"> • User input and provide the value. • Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Search Video	Video name	Provide the video name.
Download video	Downloaded file name	Provide the file name.
	Downloaded file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Upload Video	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Delete Video	N/A	N/A

Application Action	Action Parameters	Parameter Description
Like Video	N/A	N/A
Unlike Video	N/A	N/A
Logout	N/A	N/A
<i>Vkontakte</i>		
Load Login page	N/A	N/A
Login	Username	Provide the user name.
	Password	Provide the password.
View Feed	View feed message	Provide the message.
Post Message	Post message	Provide the message.
Logout	N/A	N/A
<i>Yammer</i>		
Select First Group	User email address	Provide the email address.
	User name	Provide the user name.
Select Second Group	User email address	Provide the email address.
Select Third Group	User email address	Provide the email address.
Like an Entry	User email address	Provide the email address.
Reply to a Post	User email address	Provide the email address.
	User name	Provide the user name.
Post New Message	User email address	Provide the email address.
	User name	Provide the user name.
Select Another Group	User email address	Provide the email address.

Application Action	Action Parameters	Parameter Description
<i>YYLive</i>		
Load Home Page	N/A	N/A
Select Category	Category	Provide the category.
Play Video	Video ID	Provide the Video ID.

The difference between Dynamic and Payload files

- If the chosen file is Payload (not Dynamic), the exact contents of the file can be seen on the wire.
- If the chosen file is Dynamic and the file does not contain Macros, then the behavior is the same as above.
- If the chosen file is Dynamic and the file contains Macros, then each Macro is evaluated during the test with the expected value that the Macro is meant to generate.

Artifacts

This section contains useful information and details on Playlist and Macro features.

Rules and Grammar for Playlists

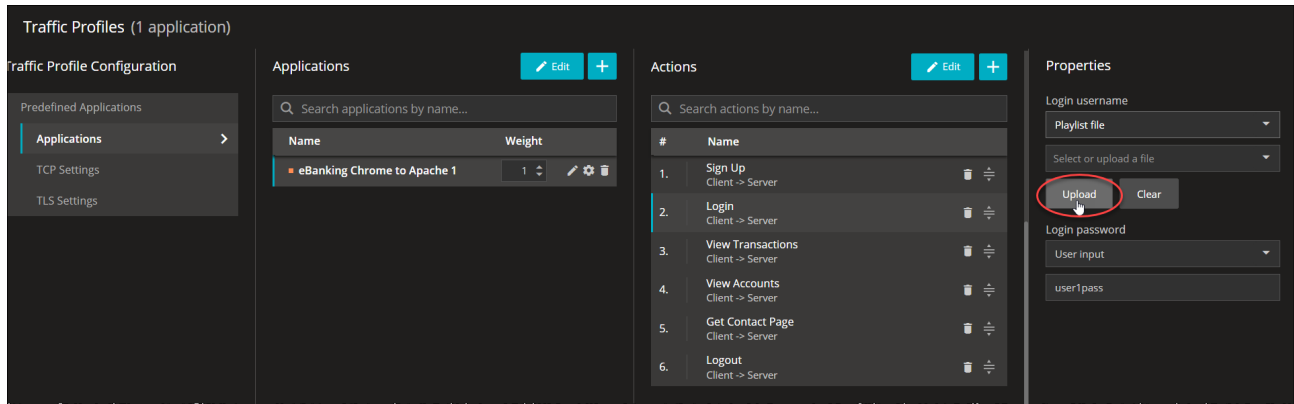
Rules to support comma or double-quotes as a part of a playlist:

1. Each playlist item with comma or double-quote in the content **must** be enclosed within double-quotes.
2. Every double-quote used as a part of the content must be escaped with another double-quote.

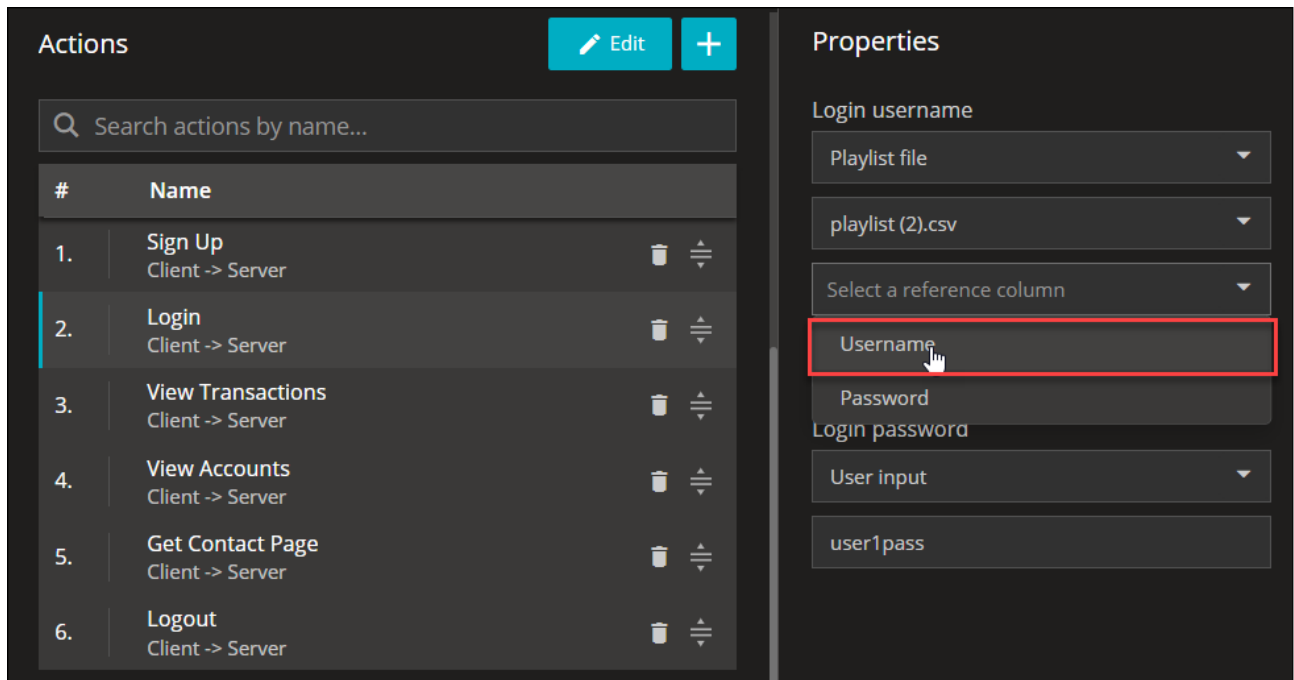
Each record is located on a separate line, delimited by a line break (CRLF). For example: `record = value *(COMMA value):`

Record	value 1	value 2
abcd	abcd	
abcd,xyz	abcd	xyz
"abcd,pqr","xyz"	abcd,pqr	xyz
"abcd,pq""r","xyz"	abcd,pq"r	xyz

For all applications that have a **Sign In** or **Sign Up** action, the following parameters offer the possibility of uploading a playlist file: Login Username, Login password or SignUp Username, SignUp password, SignUp confirm password. Select the **Playlist file** option and select the **Upload** option:



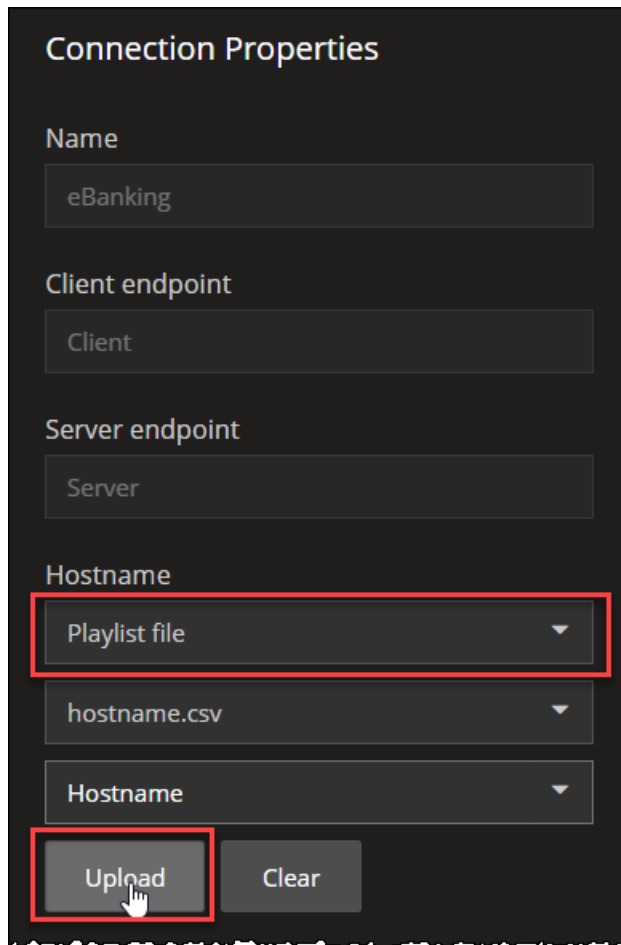
After the upload is performed, the reference column has corresponding csv column names, which can be chosen from the dropdown menu:



For some applications, the Hostname (under **ConnectionProperties**) offers the possibility of uploading a playlist file:

1. Select the **Playlist** file option .
2. Select **Upload**.

3. Choose the **Reference** column name from the drop-down.



Connection Properties

Name
eBanking

Client endpoint
Client

Server endpoint
Server

Hostname
Playlist file ▼

hostname.csv ▼

Hostname ▼

Upload Clear

Example of a Hotsname playlist file:

NOTE

As of now, we do not validate empty Hotsname values, if they are fetched from a playlist file.

	A	B
1	Hostname	
2	server1.com	
3	server2.com	
4	server3.com	
5	server4.com	
6	server5.com	
7	server6.com	
8	server7.com	
9	server8.com	
10	server9.com	
11	server10.com	
12		
13		
14		
15		
16		
17		

hostname(4107)

About Playlists

For the **Sign In** action in eBanking, eShop, Social Network, Portal or the **Sign Up** action in eBanking applications, please use this [Sign In playlist](#) file:

AutoSave Off Sign In playlist - Excel

File Home Insert Draw Page Layout Formulas Data Review View

Cut Copy Paste Format Painter Clipboard

Calibri 11 A A B I U Font

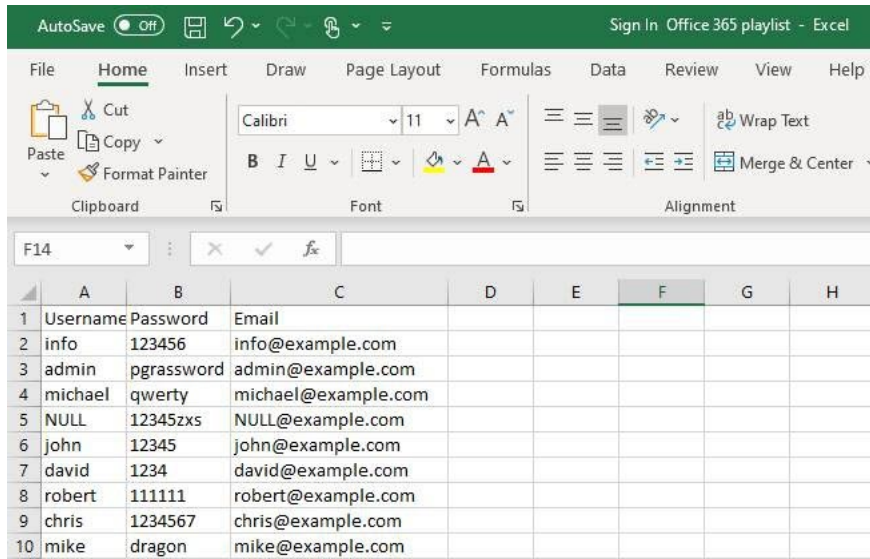
Alignment

Wrap Text Merge & Ce

P10

	A	B	C	D	E	F	G	H	I
1	Username	Password							
2	admin	pgrassword							
3	michael	qwerty							
4	NULL	123456789							
5	john	12345							

For the **Sign In** action in Office 365 (Outlook, Excel, OneDrive) applications , please use this [Sign In Office 365 playlist](#) file:



About Macros

A macro is a method or function which allows you to customize the payload text data with the following parameters. The `maxLength` limit is set to 1024:

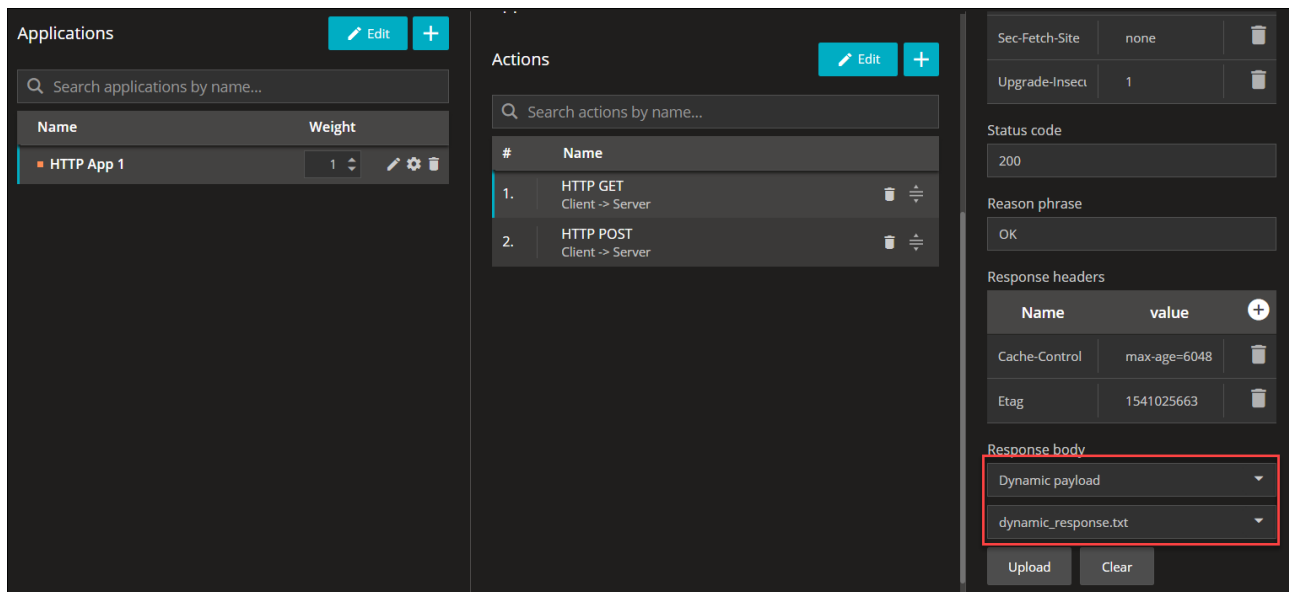
Macros	Description
<code>\$(RandomIPAddress, 'IPv4')</code>	The RandomIPAddress macro randomly generates IPv4 address. IPv6 is not yet supported.
<code>\$(Rand, minValue, maxValue)</code>	The Rand macro generates one random number within the range [minValue, maxValue]. It takes one or two parameters. Range is 0 – N or N1 – N2.
<code>\$(RandomAscii, minLength, maxLength)</code>	The RandomAscii macro generates a sequence of random Ascii characters with values in the range: 0-127. <code>minLength</code> and <code>maxLength</code> are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomAlpha, minLength, maxLength)</code>	The RandomAlpha macro generates a sequence of random letters [A-Za-z]. <code>minLength</code> and <code>maxLength</code> are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomNum, minLength, maxLength)</code>	The RandomNum macro generates a sequence of random digits. <code>minLength</code> and <code>maxLength</code> are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomAlphaNum, minLength, maxLength)</code>	The RandomAlphaNum macro generates a sequence of random letters or digits [A-Za-z0-9]. <code>minLength</code> and <code>maxLength</code> are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.

<code>\$(RandomByte, minLength, maxLength)</code>	The RandomByte macro generates a sequence of random bytes. <code>minLength</code> and <code>maxLength</code> are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(PatternRepeat, pattern, minLength, maxLength)</code>	The PatternRepeat macro generates a sequence of characters by repeating the <code><pattern></code> pattern. <code>minLength</code> and <code>maxLength</code> are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length. If the chosen length is not an exact multiple of the length of <code><pattern></code> , the last repetition of <code><pattern></code> is truncated.

The following is the macro file structure, and please use this [macros](#) file for the correct file format:

```
dynamic_payload - Notepad
File Edit Format View Help
Random IPv4 $(RandomIPAddress, 'IPv4')
Random number between 200 and 400: $(Rand, 200, 400)
Random ascii $(RandomAscii, 10, 30)
Random alpha $(RandomAlpha, 5, 20)
RandomNum $(RandomNum, 10, 20)
Random Alpha Num $(RandomAlphaNum, 10)
Random Byte $(RandomByte, 2, 4)
Repeat pattern $(PatternRepeat, '!@#4QWEr', 5)
```

This feature is also available for the HTTP application, on both HTTP GET and HTTP POST actions, under the following parameters: Response body/Response body. Switch to the dynamic payload and upload the `dynamic_payload` file:



Assign the agents, enable capture and start the test. After the test is finished, download the captured information and you can see the payload, as set in the macro file:

Appendix B Application Actions

Apply a display filter - <Ctrl>->					
No.	Time	Source	Destination	Protocol	Length Info
16	0.099346	192.168.10.91	192.168.10.90	TCP	66 [TCP Window Update] 48737 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983045 TSecr=807789105
17	0.099359	192.168.10.91	192.168.10.90	TCP	66 [TCP Window Update] 37775 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983119 TSecr=807784865
18	0.099366	192.168.10.91	192.168.10.90	TCP	66 [TCP Window Update] 58394 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983026 TSecr=807847657
19	0.099374	192.168.10.91	192.168.10.90	HTTP	371 GET /file.txt?name1=val1 HTTP/1.1
20	0.099378	192.168.10.91	192.168.10.90	HTTP	371 GET /file.txt?name1=val1 HTTP/1.1
21	0.099378	192.168.10.91	192.168.10.90	HTTP	371 GET /file.txt?name1=val1 HTTP/1.1
22	0.099623	192.168.10.90	192.168.10.91	HTTP	590 HTTP/1.1 200 OK (text/plain)
23	0.099624	192.168.10.90	192.168.10.91	HTTP	602 HTTP/1.1 200 OK (text/plain)
24	0.099646	192.168.10.91	192.168.10.90	TCP	66 [TCP Window Update] 36116 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983171 TSecr=807846794
25	0.099651	192.168.10.91	192.168.10.90	HTTP	371 GET /file.txt?name1=val1 HTTP/1.1
26	0.099685	192.168.10.90	192.168.10.91	HTTP	582 HTTP/1.1 200 OK (text/plain)

> Frame 22: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
 > Ethernet II, Src: VMware_a6:29:b9 (00:0c:29:a6:29:b9), Dst: VMware_99:5a:02 (00:0c:29:99:5a:02)
 > Internet Protocol Version 4, Src: 192.168.10.90, Dst: 192.168.10.91
 > Transmission Control Protocol, Src Port: 80, Dst Port: 58394, Seq: 1, Ack: 306, Len: 524
 > Hypertext Transfer Protocol

Line-based text data: text/plain (12 lines)
 Random IPv4 158.243.103.228\r\n
 Random number between 200 and 400: 266\r\n
 Random ascii \016\035EY\023TeI.'!]:\034+/?\031p*}\026qI\030\024<\r\n
 Random alpha VEKzKn\r\n
 RandomNum 227499253664034\r\n
 Random Alpha Num RDTu0nLmL\r\n
 Random Byte Y♦\r\n
 Repeat pattern !@#4QwEr!@#4QwEr!@#4QwEr!@#4QwEr!@#4QwEr\r\n
 \r\n
 \r\n
 \r\n
 \r\n

Index

A

agents

- clear ownership 27
- management 25
- Network Management window 28
- ownership 24
- reboot 27
- status of 25
- tags 27

application traffic generator 94, 116, 119, 128, 163

B

bidirectional UDP traffic flow 96

C

create/delete PDU session, secondary objective 89

create/delete QoS Flows, secondary objective 87

customer assistance 3

D

DNN settings

- Full Core tests 40

E

enter/exit idle, secondary objective 86

EPS fallback 178

F

Full Core tests

- network slicing 75
- objectives 77

N

Network Management window 28

O

objectives

- Full core tests 77

P

Paging, secondary objective 85

product support 3

Q

QoS flows, settings 48

R

RAN, configuration settings 171

S

SMS, secondary objective 90

stateless UDP traffic generator 92, 143

statistics

- licensing stats 244

T

tags

- custom 27

technical support 3

traffic generators 91, 142

U

UDP stateless, traffic generator 92, 143

UE configuration settings

- Full Core tests 56



© Keysight Technologies, 2023

This information is subject to change
without notice.

www.keysight.com