

LoadCore

Release 3.2

User Guide

Notices

Copyright Notice

© Keysight Technologies 2019–2022

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

Warranty

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

Technology Licenses

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

U.S. Government Rights

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

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

Contacting Us

Keysight headquarters

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

Support

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

Table of Contents

Contacting Us	3
Chapter 1 Introduction	17
Chapter 2 Licensing Requirements	18
Chapter 3 Web Interface	19
Recommended Browsers	20
Access LoadCore Web UI	20
LoadCore Web UI	20
Chapter 4 How Do I...	22
Configure and run a test	23
Create test scenarios	27
Work with saved test configurations	27
Licensed Test Configs	33
Work with test results	50
View statistics and events	50
Upgrade the MiddleWare VM	51
Configure Dashboard general settings	53
Configure LoadCore with LDAP/AD	56
Reset Password for Regular Users	60
Chapter 4 License Manager	63
Chapter 5 Traffic agents assignment and management	65
Chapter 6 Full Core tests: configuration settings	71
Global Settings	78
Global Settings panel	80
DNS Settings	80
Advanced Settings	81
DNNs panel	85

DNN configuration settings	86
Session AMBR configuration settings	89
ePCO configuration settings	90
Traffic Control Settings configuration	90
Impairment	91
QoS Flows panel	92
QoS Flow configuration settings	93
QoS Flow Packet Filter configuration settings	96
QoS Flow Max Packet Loss Rate settings	97
QoS Flow ARP configuration settings	97
QoS Flow MBR configuration settings	98
QoS Flow GBR configuration settings	98
AUSF configuration settings	99
AUSF Ranges panel	100
AUSF Range panel	100
AUSF node settings	101
AUSF Nausf interface settings	102
AUSF Remote SBA Nodes	103
AMF configuration settings	105
AMF Ranges panel	106
AMF Range settings	107
AMF node settings	108
AMF N2 interface settings	111
AMF Namf interface settings	112
AMF N26 Interface Settings	112
AMF remote SBA nodes	113
DN configuration settings	118
DN Ranges panel	119
DN Range panel	119
DN N6 interface settings	120
DN UE routes settings	121

DN User Plane	121
DN Application Traffic Generator	122
DN Stateless UDP Traffic Generator	129
MME configuration settings	131
MME Ranges panel	132
MME Range panel	132
MME node settings	134
MME S11 Interface Settings	135
MME N26 Interface Settings	136
MME S1 Interface Settings	137
MME S6a Interface Settings	139
MME Diameter	140
NRF configuration settings	141
NRF Ranges panel	142
NRF Range panel	142
NRF node settings	143
NRF Nnrf interface settings	144
SCP configuration settings	144
SCP Ranges panel	145
SCP Range panel	145
SCP interface settings	146
SCP Remote SBA Nodes	147
NSSF configuration settings	149
NSSF Ranges panel	150
NSSF Range panel	150
NSSF node settings	151
Nnssf Interface Settings	152
Remote SBA nodes	153
NSSF Restricted NSSAIs	154
NSSF Network Slices	155
NSSF Configured NSSAI	156

PCF/PCRF configuration settings	157
PCF Ranges panel	158
PCF Range panel	159
PCF node settings	160
PCRF node settings	161
PCF service area restrictions	161
PCF Npcf interface settings	162
PCRF Rx interface settings	163
PCF remote SBA nodes	164
RAN configuration settings	166
gNodeB	167
gNodeB Ranges panel	168
gNodeB Range settings	172
gNodeB node settings	173
gNodeB NSSAI settings	174
gNodeB N2 interface settings	175
gNodeB N3 interface settings	177
eNodeB	179
eNodeB Ranges panel	180
eNodeB Range Settings	180
eNodeB Node Settings	181
S1 Interface Settings	182
S1-U Interface Settings	183
Passthrough interface settings	185
SGW configuration settings	187
SGW Ranges panel	188
SGW Range panel	188
SGW S1-U Interface Settings	190
SGW S5-C Interface Settings	191
SGW S5-U Interface Settings	192
SGW S11 Interface Settings	193

SGW DUT S11 Interface Settings	194
SMF/PGW-C configuration settings	195
SMF/PGW-C Ranges panel	196
SMF/PGW-C Range settings	197
SMF node settings	198
SMF N4 interface settings	199
SMF Nsmf interface settings	200
SMF remote SBA nodes	201
NEF configuration settings	204
NEF Ranges panel	204
NEF Range panel	205
NEF Nnef interface settings	206
NEF Remote SBA Nodes	206
UDM/HSS configuration settings	209
UDM/HSS Ranges panel	210
UDM/HSS Range panel	211
UDM/HSS node settings	211
UDM/HSS Nudm interface settings	215
UDM/HSS Remote SBA Nodes	216
UDR configuration settings	218
UDR Ranges panel	218
UDR Range panel	218
UDR Nudr interface settings	219
UDR Remote SBA Nodes	220
IMS configuration settings	221
CSCF Range panel	221
CSCF N6 interface settings	222
CSCF Rx interface settings	223
CSCF UE routes settings	224
CSCF remote SBA nodes	224
Media Function Range panel	225

UPF/PGW-U configuration settings	226
UPF/PGW-U Ranges panel	227
UPF/PGW-U Range panel	227
UPF N3 interface settings	228
UPF N4 interface settings	229
UPF N6 interface settings	231
UPF N9 interface settings	231
SMSF configuration settings	234
SMSF Ranges panel	234
SMSF Range panel	235
SMSF node settings	235
SMSF Nsmsf interface settings	236
SMSF Remote SBA Nodes	237
5G-EIR configuration settings	238
5G-EIR Ranges panel	238
5G-EIR Range panel	238
5G-EIR node settings	239
5G-EIR N5g-eir interface settings	239
5G-EIR Remote SBA Nodes	240
UE configuration settings	242
UE Ranges panel	243
UE Range panel	244
Range Settings	246
UE Identification settings	247
UE Security settings	247
UE Settings settings	249
UE Shared Data IDs	253
UE Subscribed AMBR settings	253
Service Area Restriction settings	253
Forbidden Areas	255
DNNs Config	256

Notifications	257
SMS Configuration	258
Equipment Status	259
Network Slicing settings	260
UE NSSAI settings	261
UDM Default NSSAI settings	262
UDM SNSSAI Mappings	262
UDR SNSSAI Settings	263
Objectives	264
Control Plane Objective	265
About primary objectives	266
Primary Control Plane Objective	268
Secondary Control Plane Objective	270
User Plane Objectives	279
Stateless UDP Traffic	280
Data Traffic	281
Voice Traffic	284
Video OTT Traffic	287
DNS Client Traffic	290
Predefined Applications Traffic	293
NF Discovery service	304
Chapter 7 NG-RAN Simulation tests	306
Chapter 8 SBA tests: configuration settings	307
SBA Tester overview	311
SBA Tester Global Settings panel	312
Connection Settings	314
Advanced Settings	314
Impairment	316
DNNs panel	317
DNN configuration settings	318
DNN GBR configuration settings	320

Session AMBR configuration settings	320
QoS Flows panel	321
QoS Flow configuration settings	322
QoS Flow Packet Filter configuration settings	324
QoS Flow Maximum Packet Loss configuration settings	325
QoS Flow ARP configuration settings	325
QoS Flow MBR configuration settings	326
QoS Flow GBR configuration settings	326
SBA Tester Simulated Nodes panel	327
AMF configuration settings	327
SMF configuration settings	330
PCF configuration settings	333
SBA Tester Remote SBA Nodes	335
SBA Tester Remote Nodes	336
NRF configuration settings	337
NRF Ranges panel	338
NRF Range panel	338
NRF node settings	339
NRF Nnrf interface settings	340
SCP configuration settings	341
SCP Ranges panel	341
SCP Range panel	342
SCP interface settings	343
SCP Remote SBA Nodes	343
AUSF configuration settings	345
AUSF Ranges panel	346
AUSF Range panel	346
AUSF node settings	347
AUSF Nausf interface settings	348
AUSF remote SBA nodes	349
PCF configuration settings	351

PCF Ranges panel	351
PCF Range panel	352
PCF node settings	353
PCF service area restrictions	353
PCF Npcf interface settings	355
PCF remote SBA nodes	356
UDR configuration settings	356
UDR Ranges panel	356
UDR Range panel	357
UDR Nudr interface settings	358
UDR remote SBA nodes	359
UDM configuration settings	359
UDM Ranges panel	359
UDM Range panel	360
UDM node settings	361
UDM Nudm interface settings	364
UDM remote SBA nodes	365
CHF configuration settings	365
CHF Ranges panel	366
CHF Range panel	366
CHF node settings	367
CHF Nchf interface settings	367
CHF remote SBA nodes	368
NSSF configuration settings	370
NSSF Ranges panel	371
NSSF Range panel	371
NSSF node settings	372
Nnssf Interface Settings	373
Remote SBA nodes	374
NSSF Restricted NSSAIs	375
NSSF Network Slices	376

NSSF Configured NSSAI	377
UE configuration settings	378
UE Ranges panel	379
UE Range panel	379
Range Settings	380
UE Identification	381
UE Security	381
UE Settings	383
UE SDF settings	384
Shared Data IDs	385
UE Subscribed AMBR settings	385
Service Area Restrictions	385
Forbidden Areas	386
Notifications	387
Network Slicing	388
UDM Default NSSAI settings	389
UDM SNSSAI Mappings	389
UDR SNSSAI Settings	390
Charging Function	390
Policy Counters	391
Notify Policy Counters	392
Objectives	394
Primary Objective	395
About primary objectives	396
Active subscribers	398
Subscribers per Second	403
Secondary Objectives	408
UEGetNSSAIAMF2UDM	409
RegistrationAMF2UDM	410
DeregistrationAMF2UDM	411
GetPolicyAMF2PCF	412

UpdatePolicyAMF2PCF	413
GetPolicySMF2PCF	415
UpdatePolicySMF2PCF	416
RegistrationSMF2UDM	418
DeregistrationSMF2UDM	419
IntermediateSpendingLimitPCF2CHF	419
Chapter 9 UPF Isolation tests: configuration settings	421
Global Settings panel	424
DNS Settings	425
Advanced Settings	425
Impairment	428
QoS Flows panel	429
QoS Flow configuration settings	429
Reporting Settings	431
UE configuration settings	432
UE Ranges panel	433
UE Range panel	434
UE range settings	435
Objectives	440
Control Plane Objective	440
About primary objectives	441
Primary Control Plane Objective	443
Secondary Control Plane Objectives	445
User Plane Objectives	453
Stateless UDP Traffic Generator	455
Data Traffic	456
Voice Traffic	458
DNS Client Traffic	461
Video OTT Traffic	464
Predefined Applications Traffic	467
SMF configuration settings	478

SMF Ranges panel	479
SMF Range settings	479
SMF N4 interface settings	480
SMF Uplink Paths	482
RAN configuration settings	483
RAN Ranges panel	484
RAN Range settings	484
RAN N3 interface settings	485
Passthrough interface settings	486
UPF configuration settings	487
UPF Ranges panel	488
UPF Range panel	488
UPF N3 interface settings	489
UPF N4 interface settings	490
UPF N6 interface settings	492
UPF N9 interface settings	493
UPF N4u interface settings	494
DN configuration settings	497
DN Ranges panel	497
DN Range panel	497
DN N6 Interface settings	498
DN UE routes settings	499
DN User Plane	500
DN Application Traffic Generator	500
DN Stateless UDP Traffic Generator	507
Chapter 10 Passthrough testing	509
Overview of passthrough testing	510
Passthrough test configuration notes	511
Chapter 11 Troubleshooting	513
Appendix A 5G abbreviations	515
Appendix B Predefined Applications	521

Appendix C Application Actions	535
Index	585

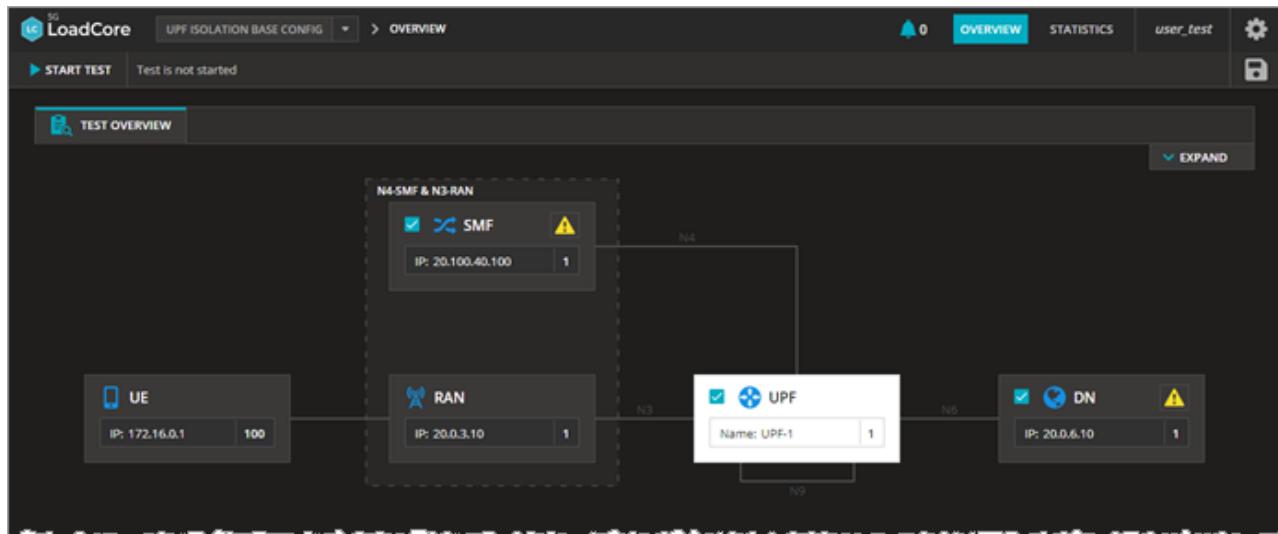
CHAPTER 1

Introduction



LoadCore simulates real-world subscriber models, enabling carriers and network equipment manufacturers to check the performance and reliability of data services on 5G Core (5GC) networks. Centered around realistic UE behavior simulation in various 5G deployments, several test topologies are available. You can alternatively deploy a full 5GC topology or opt for node isolation, interface testing, or service validation. Using the web-based interface, you can configure and execute capacity tests, detail a device's throughput, and model a wide variety of mobility scenarios.

Example test topology window for a UPF isolation test:



CHAPTER 2

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://10.38.156.169:7443/#Licenses>)

.

You can:

- activate licenses by selecting the **Activate** button or,
- deactivate Licenses by selecting the **Deactivate** button.

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

CHAPTER 3

Web Interface

The **LoadCore** solution offers a simple Web UI that allows users to configure and run tests on their 5G network and also to manage tests results .

In this chapter:

Recommended Browsers	20
Access LoadCore Web UI	20
LoadCore Web UI	20

Recommended Browsers

Only Chrome and Chrome-based browsers are supported in this release.

Access LoadCore Web UI

To log in to the LoadCore browser-based Web UI:

1. Open a supported web browser. For more details, refer to [Recommended Browsers above](#).
2. Type the `https://<IP address>` into the browser's URL. This is the IP address of the deployed middleware machine. The LoadCore log in page appears.

NOTE

If you are logging in for the first time, you are required to register and create a new user.

3. Type the username and password of your LoadCore login account.

NOTE

If you want the browser to automatically fill in the **Username** and **Password** fields for future logins, select the **Remember Me** check-box.

4. Select **Log In**. The LoadCore Dashboard page appears.

NOTE

If you are logging in for the first time, you are required to accept Keysight's Software End User License Agreement before you can log in.

LoadCore Web UI

After a successful authentication, the Dashboard page opens. On the top-right side of the Dashboard page, the user currently logged in LoadCore is displayed.

The LoadCore dashboard is split into several sections from where you can initiate and configure new tests or just manage previously configured test sessions and their results.

The following sections are displayed on the LoadCore Dashboard:

Section	Description
Settings Menu	<p>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:</p> <ul style="list-style-type: none"> • Administration - select this option to manage the settings for the following: <ul style="list-style-type: none"> ▪ License Manager - for more details, refer to License Manager. ▪ Agent Management - for more details, refer to Traffic agents assignment and management on page 65. ▪ Access Control - for more details refer to Dashboard General Settings. ▪ Software Updates - for more details, refer to Dashboard General Settings. • Application settings - select this option set or update the license server IP. For more details, refer to Dashboard General Settings. • Collect diagnostics - for more details refer to Dashboard General Settings. • Rest API Browser - select this option to open LoadCore API browser.

Section	Description
	<ul style="list-style-type: none"> • Rest API -select this option to access LoadCore Rest API reference guide. • Themes - select this option to change the LoadCore Dashboard theme. For more details, refer to Dashboard General Settings. • Help - this option displays the following: <ul style="list-style-type: none"> ▪ EULA - select this option to revisit and accept Keysight Software End User License agreement. ▪ About - this option displays details regarding the LoadCore software version. You can also access your REST API Key. The key can be copied and re-used for further purposes. For more details, refer to Dashboard General Settings. • Logout - select this option to log out of LoadCore. For more details, refer to Dashboard General Settings.
Test sessions	This section displays your current test sessions. Each test session can be accessed by selecting it.
Create New Test	<p>This sections allows you to create test sessions based on your test objectives.</p> <p>To create a new test session, select one of the following options:</p> <ul style="list-style-type: none"> • Wireless Full Core • Wireless UPF Isolation • Wireless SBA • Wireless NG-RAN Simulation <p>Selecting one of the options above will create a new session with that type of topology loaded.</p>
Browse Configs	<p>This sections allows you to manage previously configured test sessions.</p> <p>By selecting the Browse Configs button, you can perform additional test related actions:</p> <ul style="list-style-type: none"> • open a new base configuration test • delete test configurations • save test configurations • import and export test configurations <p>This section contains base test configurations plus previously loaded configurations. If you access one of the configurations (by selecting it), a new session is created with this configuration loaded inside of it.</p>
Browse Results	This sections allows you to access previous sessions results, view detailed reports and export results.
Online resources	This section contains links to the official LoadCore documentation.

CHAPTER 4

How Do I...

IMPORTANT

All the procedures presented in this section assume that you have successfully logged in to LoadCore. For more details, refer to [Access LoadCore Web UI on page 20](#).

You can perform the following actions from LoadCore:

Configure and run a test	23
Create test scenarios	27
Work with saved test configurations	27
Licensed Test Configs	33
Work with test results	50
View statistics and events	50
Upgrade the MiddleWare VM	51
Configure Dashboard general settings	53
Configure LoadCore with LDAP/AD	56
Reset Password for Regular Users	60

Configure and run a test

Based on your test objectives, you can perform the following test types:

- [Configure a Wireless Full Core test below](#)
- [Configure a Wireless UPF Isolation test on the facing page](#)
- [Configure a Wireless SBA test on page 25](#)
- [Configure and run a test above](#)

IMPORTANT

It is recommended that you decide on an IP addressing scheme before you start configuring a test. Otherwise, you can determine the IP addressing as you configure the test settings. Although you may choose to completely configure each node one at a time (including IP addresses), it is recommended that you start by configuring the IP addresses for the entire test topology. Because the 5G Core includes a large number of interfaces, systematically configuring them all at once tends to be less error-prone than configuring the addresses while configuring the other test settings.

Configure a Wireless Full Core test

To configure this test, do the following:

1. On the LoadCore Dashboard page, under the Create New Test section, select **Wireless Full Core**.
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 on page 78](#).
3. Select the services and nodes that the LoadCore 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). LoadCore 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 selecting the **Device Under Test** check box, that node will no longer be simulated by our LoadCore. You still need to configure the IP addresses of the DUT so the nodes simulated by LoadCore know who they need to communicate with.

For each node configuration, refer to its dedicated section, as follows:

- [Authentication Server Function \(AUSF\)](#)
- [Data Networks \(DN\)](#)
- [Radio Access Network \(RAN\)](#)
- [Network Repository Function \(NRF\)](#)
- [Service Communication Proxy \(SCP\)](#)
- [Unified Data Management \(UDM/HSS\)](#)

- [Unified Data Repository \(UDR\)](#)
- [Network Exposure Function \(NEF\)](#)
- [User Plane Function \(UPF/PGW-U\)](#)
- [Policy Control Function \(PCF/PCRF\)](#)
- [Access and Mobility Management Function \(AMF\)](#)
- [Network Slice Selection Function \(NSSF\)](#)
- [Short Message Service Function \(SMSF\)](#)
- [Session Management Function \(SMF/PGW-C\)](#)
- [Equipment Identity Register \(5G-EIR\)](#)
- [IP Multimedia Subsystem \(IMS\)](#)
- [Mobility Management Entity \(MME\)](#)
- [Serving Gateway \(SGW\)](#)

5. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic agents assignment and management on page 65](#).
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, LoadCore begins the registration procedure, any other configuring or occurring control plane procedure and traffic generation.
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.

Configure a Wireless UPF Isolation test

To configure this test, do the following:

1. On the LoadCore Dashboard page, under the Create New Test section, select **Wireless UPF Isolation**. 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 on page 424](#).

3. Select the services and nodes that the LoadCore 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). LoadCore 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 selecting the **Device Under Test** check box, that node will no longer be simulated by our LoadCore. You still need to configure the IP addresses of the DUT so the nodes simulated by LoadCore know who they need to communicate with.

For each node configuration, refer to its dedicated section, as follows:

- [Radio Access Network \(RAN\)](#)
- [Data Networks \(DN\)](#)
- [User Plane Function \(UPF\)](#)
- [Session Management Function \(SMF\)](#)

5. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic agents assignment and management on page 65](#).

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, LoadCore begins the registration procedure, any other configuring or occurring control plane procedure and traffic generation.

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.

Configure a Wireless SBA test

To configure this test, do the following:

1. On the LoadCore Dashboard page, under the Create New Test section, select **Wireless SBA**. 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 [SBA Tester Global Settings panel on page 312](#).

3. Select the services and nodes that the LoadCore 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). LoadCore will simulate these elements during testing.
4. Configure the test settings for the tested 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 selecting the **Device Under Test** check box, that node will no longer be simulated by our LoadCore. You still need to configure the IP addresses of the DUT so the nodes simulated by LoadCore know who they need to communicate with.

For each node configuration, refer to its dedicated section, as follows:

- [Authentication Server Function \(AUSF\)](#)
- [Unified Data Management \(UDM\)](#)
- [Unified Data Repository \(UDR\)](#)
- [Policy Control Function \(PCF\)](#)
- [Network Repository Function \(NRF\)](#)
- [Service Communication Proxy \(SCP\)](#)
- [Network Slice Selection Function \(NSSF\)](#)
- [Charging Function \(CHF\)](#)

5. Configure the test settings for the SBA tester node and simulated nodes. For more details, refer to [SBA tests: configuration settings on page 307](#).
6. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic agents assignment and management on page 65](#).
7. 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 \(UE\)](#).
8. 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.
9. Start the test. When you click or tap the **Start Test** button, LoadCore begins PDU session establishment and traffic generation.
10. a. Evaluate the results.
Once the test is running, you can click or tap **Statistics** to start monitoring the progress of the test.

TIP

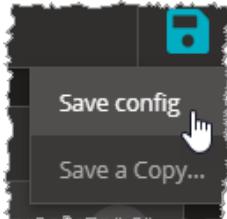
If there are multiple test sessions, you can quickly switch between them by selecting the small green triangle next to the name of the current test session. A drop-down list will displays all your current test sessions and allows you to change to a specific test session by selecting it.

Create test scenarios

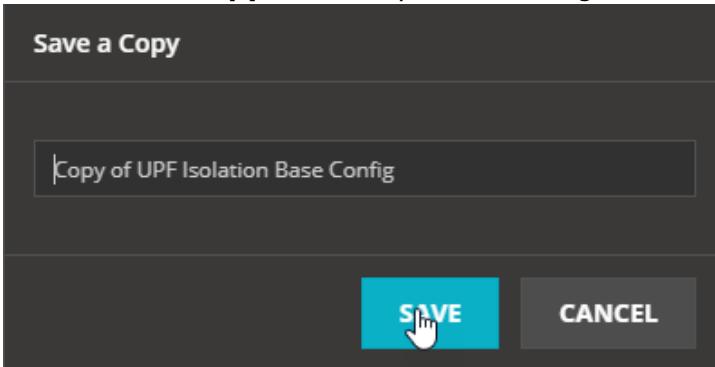
Once a test is configured (for details, refer to [Configure and run a test on page 23](#)), you can record its configuration as a scenario, edit and save it for future use.

To save a configuration file, do the following:

1. Select the **Save** icon from the upper-right corner of the Test Scenario page.



2. Select **Save config** to quickly save your test configuration.
3. Select **Save a Copy...** to save your test configuration with a specific name.



4. Provide the name for the test configuration in the Save a Copy window and select **Save**.

Work with saved test configurations

This topic describes how to work with saved test configurations.

- [The Browse Configs dashboard on the facing page](#)
- [Import a saved test configuration from disk on page 32](#)
- [Create a test session based on licensed test configuration](#)
- [Delete a saved test configuration on page 32](#)
- [Export a saved test configuration on page 32](#)

The Browse Configs dashboard

Managing saved tests is done on to Browse Configs dashboard. To access the dashboard, select the **Browse Configs** button from the main LoadCore Dashboard.



This section 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.

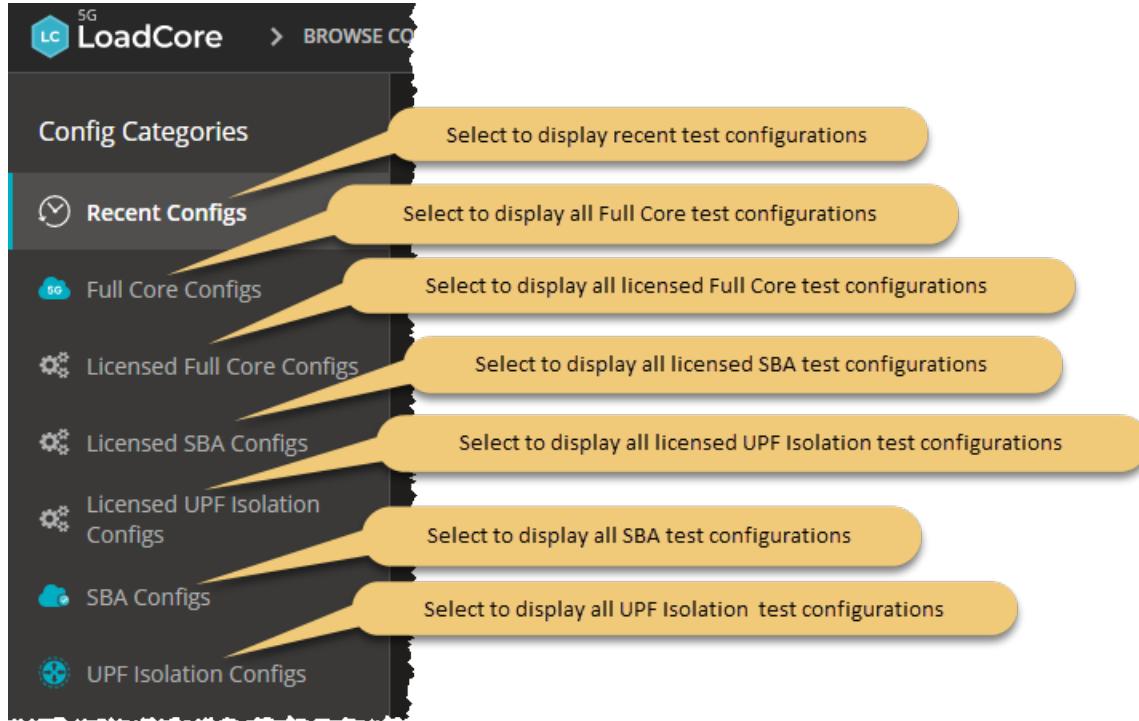
NOTE If the selected configuration is already opened in an existing session, a message is displayed allowing you to open that session or to create a new session based on the selected test configuration.

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

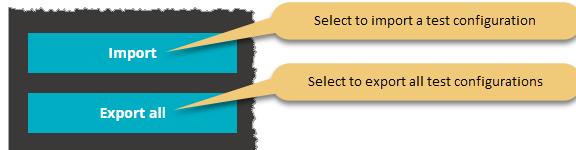
- [Test configuration categories below](#)
- [Test configuration areas on the next page](#)

Test configuration categories

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



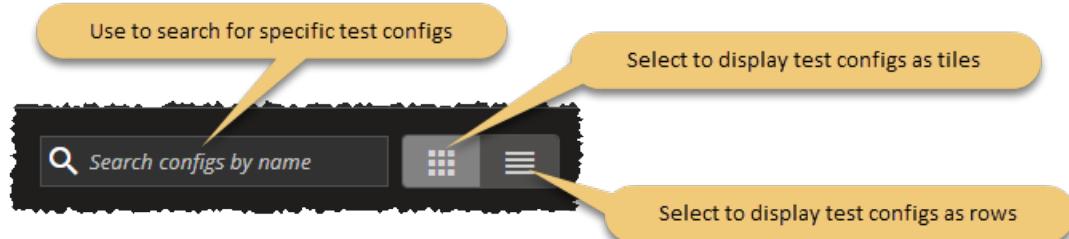
Also, you can add test configurations on the dashboard by importing them or export the existing ones.



Test configuration areas

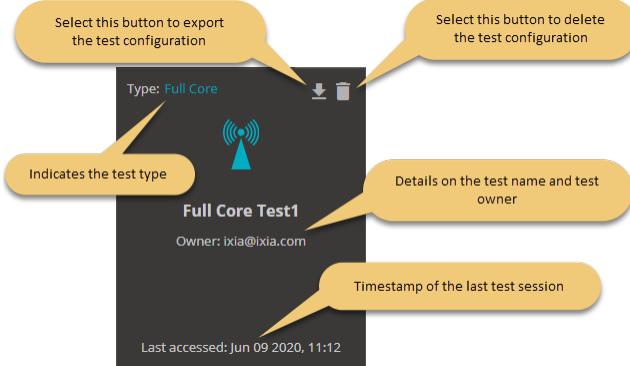
On this area, LoadCore displays your test configurations suite, offering you details on the specific test configuration and allowing you to delete it or to export it.

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



For example ...

A test configuration displayed as a tile:



Test configurations displayed as rows:

Config Name	Details on the test name	Last-accessed ↓	Application	Config Type	Owner	Create Session
<input type="checkbox"/> pdnv4 + http-get + 2MB page size + IxStack over DPDK (copy from Nov 24 15:52:16)		Nov 24, 2021, 6:31:52 PM	Full Core	admin@example...	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/> NG-RAN Simulation Base Config		Nov 24, 2021, 6:18:34 PM	Full Core	system	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/> pdnv4 + http-get + 2MB page size + IxStack over DPDK (copy from Nov 24 15:54:14)		Nov 24, 2021, 5:54:15 PM				Select to create a test session based on this configuration
<input type="checkbox"/> pdnv4 + http-get + 2MB page size + IxStack over DPDK (copy from Nov 24 15:08:23)		Nov 24, 2021, 5:08:24 PM				<input type="checkbox"/>

Use to select a test configuration

Indicates a base configuration

Timestamp of the last test session

Indicates the test type

Indicates the test owner

Delete

Export

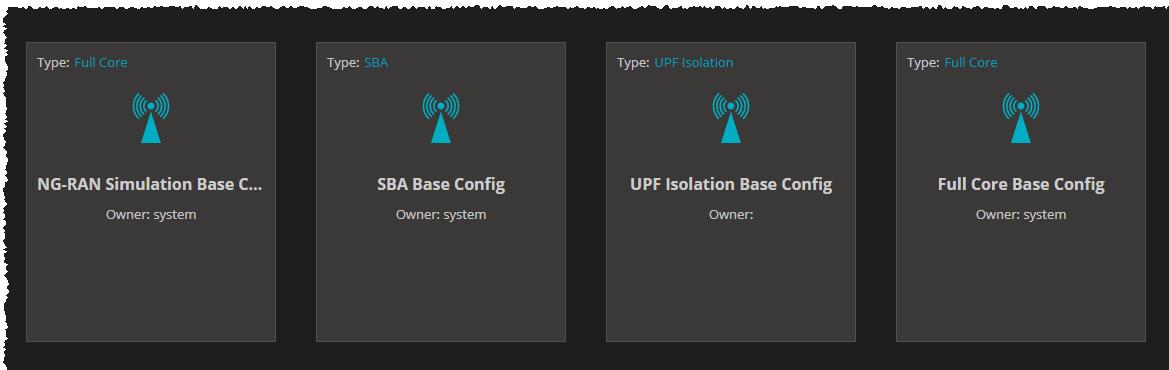
Select this button to export the test configuration

Select this button to delete the test configuration

A new wireless test has four base configurations:

- Full Core Base Config
- SBA Base Config
- UPF Isolation Base Config
- NG-RAN Simulation Base Config

For example ...



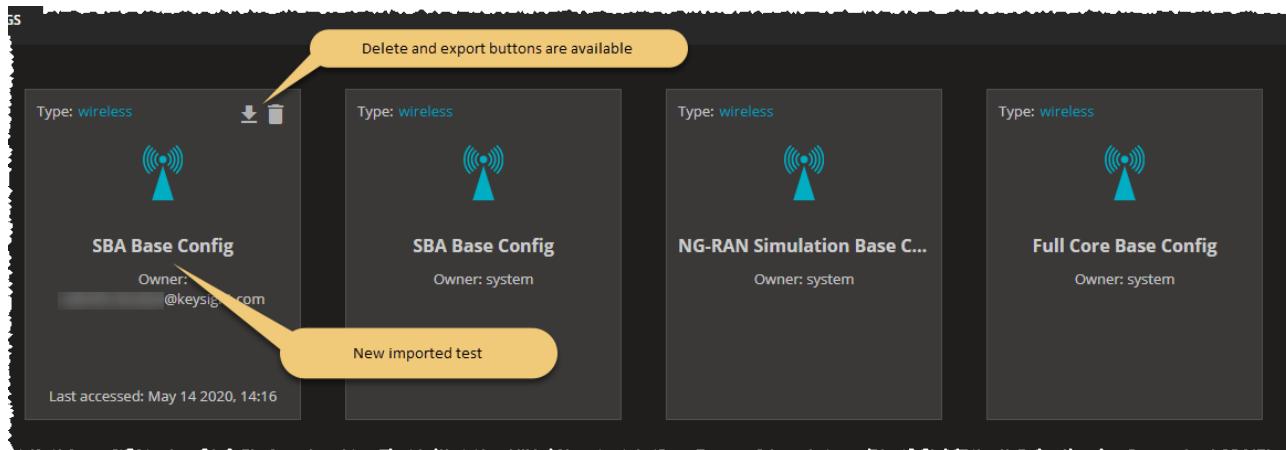
All base configurations cannot be exported or deleted, so there are no icons in the top-right corner of the test tiles and their position in the list is random. Also, for the base configurations, the test owner is *system*.

IMPORTANT

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

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

For example ...



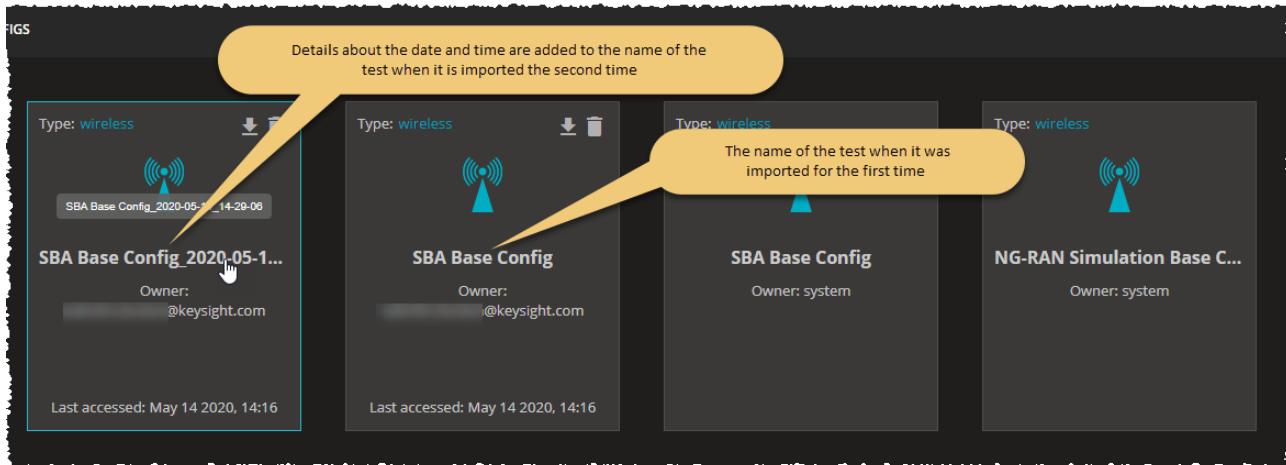
The new imported test is a user test that has the delete and export buttons on the top-right corner of the test tile.

After importing a test, the Recent Tests section will display four tests, starting from left, with the new imported test and continuing with the three base categories.

If a new test is imported, all tiles will be shifted to the right by one position, the new imported test will be the first in list and, from left to right, only four tests will be displayed. In the example above, if a new test is imported, it will be displayed first starting from left, followed by the existing imported test, SBA Base Config and NG-RAN Simulation Base Config (Full Core Base Config and UPF Isolation Base Config tests will no longer be displayed).

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.

For example ...



The same SBA test has been imported twice. Since the test was imported with the same name, the test name will be displayed with details regarding the date and time of import.

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 `displayName` is SBA Base Config. The second time it is imported, the test name is concatenated with *Imported <date> <time>*.

Import a saved test configuration from disk

To open a saved configuration, do the following:

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

Delete a saved test configuration

To delete a saved configuration, do the following:

1. From the Dashboard page, select the **Browse Tests** button. The Browse Tests page appears.
2. From the Test Categories section, select the category containing the test to be deleted.
3. From the test tile, select the **Delete** button.

Export a saved test configuration

To export a saved configuration, do the following:

1. From the Dashboard page, select the **Browse Tests** button. The Browse Tests page appears.
2. From the Test Categories section, select the category containing the test to be downloaded.
3. From the test tile, select the **Download** button.
4. Specify the download file name and select the download location.
5. Select **OK** to download the test configuration.

To export all displayed configurations, select the **Export all** button.

Licensed Test Configs

LoadCore offers a wide range of licensed test configurations for the following categories:

- [Licensed Full Core Configs](#)
- [Licensed SBA Configs](#)
- [Licensed UPF Isolation Configs](#)

Licensed Full Core Configs

The following test cases are available in the current release of LoadCore.

Test Case	Test Case Description
gNB Simulation TC 101 Single UE Reg No PDU Session SUCI Null De-Reg	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, then deregister after 1 minute without any User Plan Traffic (Control Plane Only).</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 101.1 Single UE Reg No PDU Session SUCI Null Switch Off Dereg	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, and deregister after 1 minute without any User Plan Traffic (Control Plane Only). The Deregistration Request messages will use a <i>Switch-off</i> deregistration type.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 101.2 Single UE Force Emergency Registration No PDU Session SUCI Null	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, and deregister after 1 minute without any User Plan Traffic (Control Plane Only). The registration type will be <i>Emergency registration</i> (instead of <i>Initial Registration</i>).</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 101.3 Register with 5G-GUTI and Deregister	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, and deregister after 1 minute without any User Plan Traffic (Control Plane Only). The type of user identity is set to <i>5G-GUTI</i> in <i>Registration Request</i>.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 101.4 AMF	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, and deregister after 1 minute</p>

Test Case	Test Case Description
triggers identification procedure to get UE identity during Registration	<p>without any User Plan Traffic (Control Plane Only). The AMF is expected to trigger the <i>Identification Procedure</i> to obtain the identity of the UE.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 101.5 UE registers periodic registration and then deregisters	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, and deregister after 1 minute without any User Plan Traffic (Control Plane Only). The <i>Periodic Registration Update</i> is enabled.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 101.6 Single UE in Mico mode Reg 1 PDU No UP De-Reg	<p>This test verifies that an gNB can support a single User Equipment (UE) registration without creating a PDU Session, and deregister after 1 minute without any User Plan Traffic (Control Plane Only). The UEs in the range prefer Mobile Initiated Connection Only (MICO) mode during <i>Initial Registration</i> procedure.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 102 Single UE Reg 1 PDU 1 Flow SUCI Null De-Reg UDP	<p>This test verifies that a single User Equipment (UE) can register to the 5G Core Network, can create a Protocol Data Unit (PDU) using a default QoS Flow with the Subscription Concealed Identifier (SUCI) encrypted with <i>NULL</i> profile. The UE should generate UDP traffic on the default QoS Flow and then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 104 Single UE Reg 1 PDU 1 Flow SUCI Profile B De-Reg UDP	<p>This test verifies that a single UE can register to the 5G Core Network, creates a Protocol Data Unit (PDU) using the default QoS Flow with the SUCI encrypted with the <i>Profile B</i>. The UE generates UDP traffic on the default QoS Flow and then deregisters.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 105 Single UE Reg 1 PDU 2 Flows No UP De-	<p>This test verifies that a single UE can register to the 5G Core Network, can create an PDU using a default and a dedicated QoS Flow without any User Plane Traffic (Control Plane Only). The UE will then deregister.</p> <p>This test case is available in two scenarios:</p>

Test Case	Test Case Description
Reg	<ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 106 Single UE Reg 1 PDU 2 Flows Same DNN (1x TC P 1x UDP) De-Reg	<p>This test verifies that a single UE can register to the 5G Core Network, and can create a PDU using a default and a dedicated QoS Flow on the same DNN. The UE generates UDP traffic on one QoS flow and TCP on the other QoS Flow. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 107 Single UE Reg 2 PDU 2 Flows (1x TC P 1x UDP) 2 DNN De-Reg	<p>This test verifies that a single UE can register into the 5G Core Network and can create two PDUs by using the default QoS Flow. The UE will generate UDP traffic on the first DNN, and TCP on the other DNN. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 108 Single UE Reg 2 PDU 4 Flows 2 DNN De-Reg (1x HTTP 1x HTTPS 1x UDP 1x FTP)	<p>This test verifies that a single UE can register into the 5G Core Network, and can create two PDUs and four QoS Flows (two QoS flow on one DNN, and the other two QoS flows on the second DNN). The first DNN will include two flows for HTTP and HTTPS while the second DNN will contain the other two flows for UDP and FTP traffic. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 108.1 REG and Voice Call and Deregistration	<p>This test verifies that a single User Equipment (UE) can register to the 5G Core Network, can create a Protocol Data Unit (PDU) using a default QoS Flow and generate Voice traffic on the default QoS Flow. Finally, the UE deregisters.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 108.2 Single UE with UDP and Voice traffic	<p>This test verifies that a single User Equipment (UE) can register to the 5G Core Network, can create one Protocol Data Unit (PDU) using a default QoS Flow, and generate Voice and UDP Data traffic on the default QoS Flow. Finally, the UE deregisters.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation	This test verifies that a single User Equipment (UE) can register to the 5G Core

Test Case	Test Case Description
TC 108.3 Single UE with UDP HTTP and Voice traffic	<p>Network, can create a Protocol Data Unit (PDU) using a default QoS Flow, and generate Voice and Data (both UDP and TCP/HTTP) traffic on the default QoS Flow. Finally, the UE deregisters.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 109 Single UE Reg 1 PDU 1 Flow 1 HO De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, and can create one PDU using a default QoS flow with UDP traffic generation. It also performs a single handover. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 110 Single UE Reg 1 PDU 1 Flow Multiple HO De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, and can create an PDU using a default QoS flow with UDP traffic generation. It also performs multiple handovers. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 111 Single UE Reg 2 PDU 2 Flow Multiple HO De-Reg UDP	<p>This test verifies that a single UE can register to the 5G Core Network, can create two PDUs using the default QoS flows with UDP traffic generation on both flows, while performing multiple handovers. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 112 Single UE Reg 1 PDU 1 Flow 1 Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register to the 5G Core Network, can create a PDU using the default QoS flow with UDP traffic generation. The UE then enters and exits the Idle status for one single time. The UE will then deregister from the network.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 113 Single UE Reg 1 PDU 1 Flow Multiple Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, can create a PDU using a default QoS flow with UDP traffic generation, while the UE enters and exits the Idle state multiple times. The UE will then deregister from the network.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed

Test Case	Test Case Description
	<ul style="list-style-type: none"> • B2B - DUT not deployed
gNB Simulation TC 114 Single UE Reg 2 PDU 2 Flows Multiple Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, and can create two PDUs using a default QoS flow with UDP traffic generation on both flows while performing multiple enters and exits to/from Idle state. The UE will then deregister from the network.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 115 Single UE Reg 1 PDU 1 Flow 1 HO 1 Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, can create a PDU using the default QoS flow with UDP traffic generation, while the UE performs a single handover and a single enter and exit Idle state. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 116 10 UEs Reg 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP	<p>This test verifies that 10 UEs can register into the 5G Core Network, and can create a PDU using a default QoS flow with UDP traffic generation per UE, while each of the 10 UEs perform multiple handovers and multiple enter and exit idle state at a rate of 1 per second. The UEs will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 117 10 UEs Reg Rate 1/s 1 PDU 1 Flow De- Reg	<p>This test verifies that 10 UEs can register in to the 5G Core Network at a rate of 1 per second while also creating a PDU using a default QoS flow per UE. After the hold time expires, all UEs will deregister and the test will repeat at 1 UE per second for the sustain time duration.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 118 10 UEs Reg Rate 1/s 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP	<p>This test verifies that 10 UEs register in to the 5G Core Network at a rate of one per second while also creating a PDU using a default QoS flow per UE, and generating UDP traffic on every UE. During traffic generation, the UEs will perform multiple handovers and multiple entering and exiting the idle state at a rate of 1 per second. The UEs will deregister and then repeat this process at 1 UE per second for the entire duration of the sustain time.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed

Test Case	Test Case Description
gNB Simulation TC 119 10 gNBs 10 UEs Reg 10 PDU 10 Flow No UP De-Reg	<p>This test verifies that the 5G Core Network can support 10 gNBs with 10 UEs registering to each gNB while also creating 10 PDUs and 10 QoS Flows with no user plane traffic (Control Plane Only). All UEs will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 120 10 gNBs 10 UEs Reg Rate 1/s 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP	<p>This test verifies that the 5G Core Network can support 10 gNBs with 10 UEs registering at a rate of 1 UE per second to each gNB while also creating a PDU per UE using the default QoS flow per UE with UDP traffic being generated on each of the default QoS Flows. While traffic is generated, the UEs perform multiple handovers and multiple entering and exiting idle states at a rate of 1 per second. All UEs will then deregister and repeat this process for the entire duration of the test.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 702 100UEs and 22GB-HTTP Get Traffic - withSingle Port Pair	<p>This test verifies that the 5G Core Network can support 24 gNBs with 100 UEs, each using a PDU and a QoS Flow. Traffic type will be <i>HTTP Get</i> trying to achieve 22 Gbps of the User Plane Throughput.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 703 1000UEs and 90GB-HTTP Get Traffic with FourPort Pairs	<p>This test verifies that 5G Core Network can support 48 gNBs with 1000 UEs, each using a PDU and a QoS Flow. Traffic type will be <i>HTTP Get</i> trying to achieve 90 Gbps of User Plane Throughput.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 704 1000UEs and 50GB- Data and voice traffic mix	<p>This test verifies that the 5G Core Network can support 48 gNBs with 1000 UEs, each using a PDU and a QoS Flow. The traffic type will be <i>HTTP Get – 35%, HTTPS Get – 10%, HTTP Get Port 70 – 25%, UDP Bi-Directional – 30%</i>, Voice Basic Call, trying to get 100 GB, but will achieve 50 Gbps of the User Plane Throughput.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
gNB Simulation TC 705 5000UEs	<p>This test verifies that the 5G Core Network can support 48 gNBs with 1000 UEs, each using a PDU and a QoS Flow. The traffic type will be <i>HTTP Get –</i></p>

Test Case	Test Case Description
and 50GB- Data traffic mix	<p>35%, <i>HTTPS Get</i> – 10%, <i>HTTP Get Port 70</i> – 25%, <i>UDP Bi-Directional</i> – 30%, trying to get 100 GB, but will achieve 50 Gbps of User Plane Throughput.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 101 Single UE Reg No PDU Session SUCI Null De-Reg	<p>This test verifies that an AMF can support a single User Equipment (UE) registration without creating a PDU Session, then deregister after 1 minute without any User Plan Traffic (Control Plane Only).</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 102 Single UE Reg 1 PDU 1 Flow SUCI Null De-Reg UDP	<p>This test verifies that a single User Equipment (UE) can register to the 5G Core Network, can create a Protocol Data Unit (PDU) using a default QoS Flow with the Subscription Concealed Identifier (SUCI) encrypted with <i>NULL</i> profile. The UE should generate UDP traffic on the default QoS Flow and then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 104 Single UE Reg 1 PDU 1 Flow SUCI Profile B De-Reg UDP	<p>This test verifies that a single UE can register to the 5G Core Network, creates a Protocol Data Unit (PDU) using the default QoS Flow with the SUCI encrypted with the <i>Profile B</i>. The UE generates UDP traffic on the default QOS Flow and then deregisters from the network.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 105 Single UE Reg 1 PDU 2 Flows No UP De-Reg	<p>This test verifies that a single UE can register to the 5G Core Network, can create an PDU using a default and a dedicated QoS Flow without any User Plane Traffic (Control Plane Only). The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 106 Single UE Reg 1 PDU 2 Flows Same DNN (1x TC P 1x UDP) De-Reg	<p>This test verifies that a single UE can register to the 5G Core Network, and can create a PDU using a default and a dedicated QoS Flow on the same DNN. The UE generates UDP traffic on one QoS flow and TCP on the other QoS Flow. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed

Test Case	Test Case Description
	<ul style="list-style-type: none"> • B2B - DUT not deployed
AMF Isolation TC 107 Single UE Reg 2 PDU 2 Flows (1x TCP 1x UDP) 2 DNN De- Reg	<p>This test verifies that a single UE can register into the 5G Core Network and can create two PDUs by using the default QoS Flow. The UE will generate UDP traffic on the first DNN, and TCP on the other DNN. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 108 Single UE Reg 2 PDU 4 Flows 2 DNN De- Reg (1x HTTP 1x HTTPS 1x UDP 1x FTP)	<p>This test verifies that a single UE can register into the 5G Core Network, and can create two PDUs and four QoS Flows (two QoS flow on one DNN, and the other two QoS flows on the second DNN). The first DNN will include two flows for HTTP and HTTPS while the second DNN will contain the other two flows for UDP and FTP traffic. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 109 Single UE Reg 1 PDU 1 Flow 1 HO De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, and can create one PDU using a default QoS flow with UDP traffic generation. It also performs a single handover. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 110 Single UE Reg 1 PDU 1 Flow Multiple HO De- Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, and can create an PDU using a default QoS flow with UDP traffic generation. It also performs multiple handovers. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 111 Single UE Reg 2 PDU 2 Flow Multiple HO De- Reg UDP	<p>This test verifies that a single UE can register to the 5G Core Network, can create two PDUs using the default QoS flows with UDP traffic generation on both flows, while performing multiple handovers. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 112 Single UE Reg 1 PDU 1 Flow 1 Enter/Exit Idle	<p>This test verifies that a single UE can register to the 5G Core Network, can create a PDU using the default QoS flow with UDP traffic generation. The UE then enters and exits the Idle status for one single time. The UE will then deregister from the network.</p>

Test Case	Test Case Description
De-Reg UDP	<p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 113 Single UE Reg 1 PDU 1 Flow Multiple Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, can create a PDU using a default QoS flow with UDP traffic generation, while the UE enters and exits the Idle state multiple times. The UE will then deregister from the network.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 114 Single UE Reg 2 PDU 2 Flows Multiple Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, and can create two PDUs using a default QoS flow with UDP traffic generation on both flows while performing multiple enters and exits to/from Idle state. The UE will then deregister from the network.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 115 Single UE Reg 1 PDU 1 Flow 1 HO 1 Enter/Exit Idle De-Reg UDP	<p>This test verifies that a single UE can register into the 5G Core Network, can create a PDU using the default QoS flow with UDP traffic generation, while the UE performs a single handover and a single enter and exit Idle state. The UE will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 116 10 UEs Reg 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP	<p>This test verifies that 10 UEs can register into the 5G Core Network, and can create a PDU using a default QoS flow with UDP traffic generation per UE, while each of the 10 UEs perform multiple handovers and multiple enter and exit idle state at a rate of 1 per second. The UEs will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 117 10 UEs Reg Rate 1/s 1 PDU 1 Flow De-Reg	<p>This test verifies that 10 UEs can register in to the 5G Core Network at a rate of 1 per second while also creating a PDU using a default QoS flow per UE. After the hold time expires, all UEs will deregister and the test will repeat at 1 UE per second for the sustain time duration.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed

Test Case	Test Case Description
AMF Isolation TC 118 10 UEs Reg Rate 1/s 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP	<ul style="list-style-type: none"> • B2B - DUT not deployed <p>This test verifies that 10 UEs register in to the 5G Core Network at a rate of one per second while also creating a PDU using a default QoS flow per UE, and generating UDP traffic on every UE. During traffic generation, the UEs will perform multiple handovers and multiple entering and exiting the idle state at a rate of 1 per second. The UEs will deregister and then repeat this process at 1 UE per second for the entire duration of the sustain time.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 119 10 gNBs 10 UEs Reg 10 PDU 10 Flow No UP De-Reg	<p>This test verifies that the 5G Core Network can support 10 gNBs with 10 UEs registering to each gNB while also creating 10 PDUs and 10 QoS Flows with no user plane traffic (Control Plane Only). All UEs will then deregister.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
AMF Isolation TC 120 10 gNBs 10 UEs Reg Rate 1/s 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP	<p>This test verifies that the 5G Core Network can support 10 gNBs with 10 UEs registering at a rate of 1 UE per second to each gNB while also creating a PDU per UE using the default QoS flow per UE with UDP traffic being generated on each of the default QoS Flows. While traffic is generated, the UEs perform multiple handovers and multiple entering and exiting idle states at a rate of 1 per second. All UEs will then deregister and repeat this process for the entire duration of the test.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed

Licensed SBA Configs

The following test cases are available in the current release of LoadCore.

Test Case	Test Case Description
UDM Isolation TC 101 Registration AMF to UDM	<p>This test verifies the capability of the UDM to respond to <i>Registration AMF to UDM</i>.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
UDM Isolation TC 102 Registration and	<p>This test verifies the capability of the UDM to respond to <i>Registration AMF to UDM</i> and <i>Deregistration AMF to UDM</i>.</p>

Test Case	Test Case Description
Deregistration AMF to UDM	<p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
UDM Isolation TC 103 Registration AMF to UDM and Registration SMF to UDM	<p>This test verifies the capability of the UDM to respond to <i>Registration AMF to UDM</i> and <i>Registration SMF to UDM</i>.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
UDM Isolation TC 104 Registration AMF to UDM and Registration SMF to UDM and Deregistration for both	<p>This test verifies the capability of the UDM to respond to <i>Registration AMF to UDM</i>, <i>Registration SMF to UDM</i>, <i>Deregistration AMF to UDM</i> and <i>Deregistration SMF to UDM</i>.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
UDM Isolation TC 105 UE Get NSSAI AMF to UDM	<p>This test verifies the capability of the UDM to respond to <i>Get NSSAI AMF to UDM</i>.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 101 AM Policy Association Establishment	<p>This test verifies the capability of PCF to respond to <i>Npcf_AMPolicyControl_Create</i> Service Operation. It tests the AM Policy Association Establishment as described in TS 29.513 Chapter 5.1.1.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 102 AM Policy Association Modification initiated by the AMF	<p>This test verifies the capability of PCF to respond to <i>Npcf_AMPolicyControl_Create</i> and <i>Update</i> Service Operation.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 103 SM Policy Association Establishment	<p>This test verifies the capability of PCF to respond to <i>Npcf_SMPolicyControl_Create</i> Service Operation.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed

Test Case	Test Case Description
PCF Isolation TC 104 SM Policy Association Modification initiated by the SMF	<p>This test verifies the capability of PCF to respond to <i>Npcf_SMPolicyControl_Create</i> and <i>Update</i> Service Operation.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 105 AM & SM Policy Association Establishment	<p>This test verifies the capability of PCF to respond to both <i>Npcf_AMPolicyControl_Create</i> and <i>Npcf_SMPolicyControl_Create</i> Service Operations.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 106 AM & SM Policy Association Modification initiated by the AMF	<p>This test will verify the capability of PCF to respond to <i>Npcf_AMPolicyControl_Create</i>, <i>Npcf_AMPolicyControl_Update</i>, <i>Npcf_SMPolicyControl_Create</i> and <i>Npcf_SMPolicyControl_Update</i> Service Operation.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 107 AM Policy Association Termination	<p>This test verifies that the AMF can terminate a policy sent to the PCF.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 109 SM Policy Association Termination	<p>This test verifies that the SMF can terminate a policy sent to the PCF.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 131 SM Policy Association Modification Trigger AC_TY_CH (Access Type Change)	<p>This test verifies that SMF can initiate an Update policy using the Access Type Change trigger type.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 132 SM Policy Association Modification Trigger PLMN_CH (PLMN)	<p>This test verifies that SMF can initiate an Update policy using the <i>PLMN Change</i> trigger type.</p> <p>This test case is available in two scenarios:</p>

Test Case	Test Case Description
Change)	<ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 133 SM Policy Association Modification Trigger RES_MO_RE (Resource Mod)	<p>This test verifies that the SMF can initiate an Update policy using the trigger for a request for resource modification. The SMF always reports to the PCF.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 134 SM Policy Association Modification Trigger UE_MAC_CH (MAC Change)	<p>This test verifies that the SMF can initiate an Update policy using the trigger for a new user equipment MAC address or an inactive, used UE MAC address.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 135 SM Policy Association Modification Trigger AN_CH_COR (Access Network Info)	<p>This test verifies that the SMF can initiate an Update policy using the trigger for Access Network Charging Correlation Information.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 136 SM Policy Association Modification Trigger US_RE (PDU Threshold)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when the PDU Session or the Monitoring key specific resources consumed by a UE either reach the threshold or requires reporting for other reasons.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 137 SM Policy Association Modification Trigger APP_STA (App Traffic Start)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when detecting the start of application traffic.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 138 SM Policy Association Modification Trigger APP_STO (App Traffic Stop)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when detecting the application traffic stops.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed

Test Case	Test Case Description
PCF Isolation TC 139 SM Policy Association Modification Trigger AN_INFO (Access Network Info Report)	<p>This test verifies that the SMF can initiate an Update policy using the trigger for the Access Network Information report.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 140 SM Policy Association Modification Trigger CM_SES_FAIL (Credit Session Fail)	<p>This test verifies that the SMF can initiate an Update policy using the trigger for credit management session failure.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 141 SM Policy Association Modification Trigger PS_DA_OFF (3GPP PS Data Off Change)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when the SMF reports a change in the 3GPP PS Data Off status.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 142 SM Policy Association Modification Trigger DEF_QOS_CH (Default QOS Change)	<p>This test verifies that the SMF can initiate an update policy using the trigger when the default QoS changes. The SMF always reports to PCF.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 143 SM Policy Association Modification Trigger SE_AMBR_CH (Session AMBR Change)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when the session AMBR changes. The SMF always reports to the PCF.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 144 SM Policy Association Modification Trigger QOS_NOTIF (Not Guaranteed QOS Flow)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when the SMF notifies the PCF about receiving notification from RAN that the QoS targets of the QoS Flow cannot be guaranteed, or re-guaranteed.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 145 SM	This test verifies that the SMF can initiate an Update policy using

Test Case	Test Case Description
Policy Association Modification Trigger NO_CREDIT (Out of Credit)	<p>the trigger when UEs are out of credit.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 146 SM Policy Association Modification Trigger PRA_CH (UE Presence Change)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when a change of UE presence in the Presence Reporting Area is detected.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 147 SM Policy Association Modification Trigger SAREA_CH (Serving Area Change)	<p>This test verifies that the SMF can initiate an Update policy using the trigger when a Serving Area Location Change is detected.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 148 SM Policy Association Modification Trigger SCNN_CH (Serving CN Node Change)	<p>This test verifies that the SMF can initiate an update policy using the trigger when a Serving CN Node Location Change is detected.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 149 SM Policy Association Modification Trigger RE_TIMEOUT (PCC Timeout)	<p>This test verifies that the SMF can initiate an Update policy using the trigger that indicates the SMF generated the request because a Policy and Charging Control (PCC) revalidation timeout occurred.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 150 SM Policy Association Modification Trigger RES_RELEASE (Resource Release)	<p>This test verifies that the SMF can initiate an Update policy using the trigger that indicates the SMF can inform PCF about the release of the required resources.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 151 SM Policy Association Modification Trigger SUCC_RES_ALLO	<p>This test verifies that the SMF can initiate an update policy using the trigger that indicates the requested rule data is the successful resource allocation.</p>

Test Case	Test Case Description
(Success Rule Release)	<p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 152 SM Policy Association Modification Trigger RAT_TY_CH (RAT Type Change)	<p>This test verifies that the SMF can initiate an Update policy using the trigger that indicates a RAT Type Change.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed
PCF Isolation TC 153 SM Policy Association Modification Trigger REF_QOS_IND_CH (QoS Indication Error)	<p>This test verifies that the SMF can initiate an Update policy using the trigger for a Reflective QoS indication Change.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> • Live - DUT deployed • B2B - DUT not deployed

Licensed UPF Isolation Configs

The following test cases are available in the current release of LoadCore.

Test Case	Test Case Description
TC-01 UPF Isolation 1000 UE 400Kbps Per UE 400Mbps HTTP Throughput	This test validates real UPF performance when 1000 UEs are generating 400Mbps HTTP Throughput in the DL. UE DL AMBR 400Kbps & UL 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-02 UPF Isolation 1000 UE 400Kbps Per UE 400Mbps HTTP Throughput DPI_Configured	This test validates real UPF performance when 1000 UEs are generating 400Mbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3 . UE DL AMBR 400Kbps & UL 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-03 UPF Isolation 10000 UE 400Kbps Per UE 4Gbps HTTP Throughput	This test validates real UPF performance when 10000 UEs are generating 4Gbps HTTP Throughput in the DL. UE DL AMBR 400Kbps & UL 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-04 UPF Isolation 10000 UE 400Kbps Per UE 4Gbps HTTP Throughput DPI_Configured	This test validates real UPF performance when 10000 UEs are generating 4Gbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3. UE DL AMBR 400Kbps & UL 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-05 UPF Isolation 50K UE 400Kbps Per	This test validates real UPF performance when 50K UEs are generating 20Gbps HTTP Throughput in the DL. UE DL AMBR 400Kbps & UL 10Kbps,

Test Case	Test Case Description
UE 20Gbps HTTP Throughput	QFI 5, 6, 7 used in the test to send 6PDRs.
TC-06 UPF Isolation 50K UE 400Kbps Per UE 20Gbps HTTP Throughput DPI_Configured	This test validates real UPF performance when 50k UEs are generating 20Gbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3. UE DL AMBR 400Kbps & UL 10Kbp, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-07 UPF Isolation 1 UE Max Throughput	This test validates real UPF performance with 1 super user generating 5Gbps throughput in DL. UE DL AMBR 10Gbps & UL 10Gbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-08 UPF Isolation 30K UE 2Mbps Per UE 60Gbps HTTP Throughput	This test validates real UPF performance when 30k UEs are generating 60Gbps HTTP Throughput in the DL. UE DL AMBR 2Mbps & UL 200Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-09 UPF Isolation 30K UE 2Mbps Per UE 60Gbps HTTP Throughput DPI_Configured	This test validates real UPF performance when 30k UEs are generating 60Gbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3. UE DL AMBR 2Mbps & UL 200Kbp, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-10 UPF Isolation 15K UE 5Mbps Per UE 75Gbps HTTP Throughput	This test validates real UPF performance when 15k UEs are generating 75Gbps HTTP Throughput in the DL. UE DL AMBR 5Mbps & UL 200Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-11 UPF Isolation 15K UE 5Mbps Per UE 75Gbps HTTP Throughput DPI_Configured	This test validates real UPF performance when 15k UEs are generating 75Gbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3. UE DL AMBR 5Mbps & UL 200Kbp, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-12 UPF Isolation 200K UE 300 Kbps Per UE 60Gbps HTTP Throughput	This test validates real UPF performance when 200KUEs are generating 60Gbps HTTP Throughput in the DL. UE DL AMBR 300Kbps & UL 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-13 UPF Isolation 200K UE 300 Kbps Per UE 60Gbps HTTP Throughput DPI_Configured	This test validates real UPF performance when 200k UEs are generating 60Gbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3. UE DL AMBR 300Kbps & UL 10Kbp, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-14 UPF Isolation 600K UE 100 Kbps Per UE 60Gbps HTTP	This test validates real UPF performance when 600K UEs are generating 60Gbps HTTP Throughput in the DL. UE DL AMBR 100Kbps & UL 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.

Test Case	Test Case Description
Throughput	
TC-15 UPF Isolation 600K UE 100 Kbps Per UE 60Gbps HTTP Throughput DPI_ Configured	This test validates real UPF performance when 600k UEs are generating 60Gbps HTTP Throughput in the DL with DPI feature configured using Application IDs Host1, Host2 and Host3. UE DL AMBR 100Kbps & UL 10Kbp, QFI 5, 6, 7 used in the test to send 6PDRs.

Work with 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**.



This 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 & Logs** - download an archive containing both MW and Agent logs.
- NOTE** To download the captures you need to enable traffic capture on the test agents.
-
- Delete the test results, by selecting the **Delete** button.
- NOTE** At this moment, LoadCore does not have an automatic mechanism to delete old results, therefore this operation must be done manually in order to prevent MW disk to become full (especially running long duration tests).

View statistics and events

To view statistics, select the **Statistics** tab.



The events button indicates in real-time the number of registered events. Also, by hovering over the events button, it will display the number and severity type of the recorded events.

When selected, the Events window is displayed. Here you can view details on the registered events regarding the logging date, their severity type and description. You can also customize this window by selecting/clear the check-box associated to the event severity you need to be displayed.

The screenshot shows a modal window titled "Events". At the top, there are filter checkboxes for "All", "Info", "Warning", and "Error". Below the filters is a table with three columns: "Date ↑", "Type", and "Message". A single row is visible, showing "Nov 23, 2020, 4:00:57 PM" in the Date column, "ERROR" in the Type column, and "Could not get agents" in the Message column. At the bottom of the window are two buttons: "GO TO EVENTS PAGE" and "CLOSE".

To view the events page, select the **Go to Events Page** button.

The screenshot shows the LoadCore interface with the title bar "LoadCore 5G" and "EVENTS". On the right side, there is a bell icon with the number "0" and the "Ixia" logo. Below the title bar is a search bar labeled "Filter events by" with a dropdown menu. Underneath the search bar are four input fields: "Message" (with a search icon), "From" (with a date picker), "To" (with a date picker), and "Notification type" (with checkboxes for "All", "Info", "Warning", and "Error"). Below these fields is a table with columns "Date ↑", "Type", and "Message". A single row is visible, showing "Nov 23, 2020, 4:00:57 PM" in the Date column, "ERROR" in the Type column, and "Could not get agents" in the Message column.

Here you can search for events based on the available filtering criteria. You can filter the displayed events based on keywords, on certain logging period or just by selecting the notification types you need.

Upgrade the MiddleWare VM

To upgrade the LoadCore MiddleWare VM, do the following:

1. Download the latest upgrade file from LoadCore dedicated section on Ixia's Customer Portal (<https://support.ixiacom.com/support-overview/product-support/downloads-updates>).

NOTE

If this is the first time you access Ixia Customer Portal, you will be required to create an account.

2. From the download location, copy the upgrade file (for example, `installer-w1.0.0-2431.tar`) to the root folder `/home/appsec`.
3. From the root folder `/home/appsec`, extract the upgrade file using the following command:

```
tar xvf installer-w1.0.0-2431.tar
```

The file created is `installer-w1.0.0-2431.tgz`. This file will be used to upgrade the MiddleWare VM.

4. From the root folder `/home/appsec`, delete the following file: `installer.tgz`.

NOTE

This step is not mandatory, it is intended only to save disk space.

5. To start the upgrade process, run the command: `./update.sh --update-file=installer-w1.0.0-2431.tgz`, where the `update-file` parameter takes as value the name of the upgrade file (in this case, `installer-w1.0.0-2431.tgz`).
6. After the upgrade, log into LoadCore using your authentication credentials.

Configure Dashboard general settings

Access Control

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](#).

For more details about LDAP configuration, refer to [Configure LDAP](#).

For more details about password reset for regular users, refer to [Password Reset](#).

Software Updates

This section displays info related to the current installed software version of LoadCore.

For example ...

The screenshot shows the 'SOFTWARE UPDATES' page of the LoadCore interface. It has two main sections: 'Installed Software:' and 'Ready to be installed:'.

Installed Software:		Ready to be installed:
ATI Update	KCOS Framework	There is no software ready to be installed.
22.2.621	0.31.19	
KCOS Host System	KCOS local storage	
0.21.1	0.31.19	
KCOS SSO	Keysight Load Core	
0.13.43	3.2.0-3391-232	
WAP		
1.0.5078+releaseloadcore32		

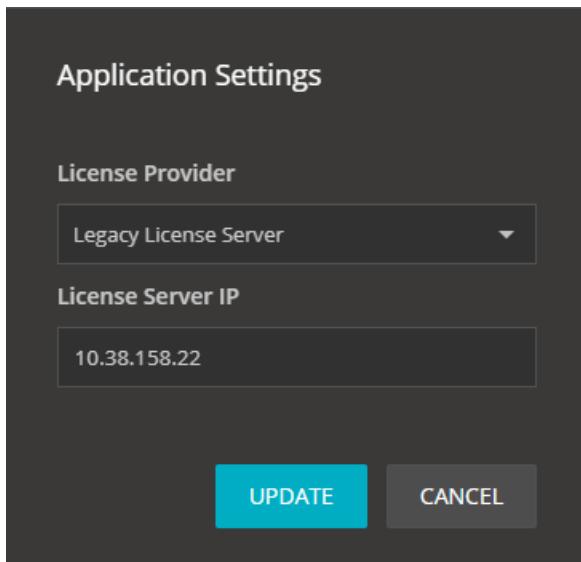
At the bottom, there are three buttons: 'Select Packages For Upload', 'Start Update', and 'Reset Current Changes'.

To update to a newer version, do the following:

1. Select the wheel icon > **Administration** > **Software Updates**.
2. Select **Select Packages For Upload** and open the folder containing the upgrade file.
3. Select the upgrade file and select **Open**.
4. Select **Start Update** to initiate the update process.
5. If needed, you can remove the update packages from the update section by selecting **Reset Current Changes**.

Application settings

This sections allows you to select the license provider and, if needed, update the license server IP address.



The following options are available for License Provider:

- **Legacy License Server** - this option is set by default on LoadCore.
- **External License Server** - select this option to set an external license server.
- **Embedded License Server** - the license server that is included in LoadCore MW. If you want to activate licenses, go to wheel icon > [Application Settings](#).

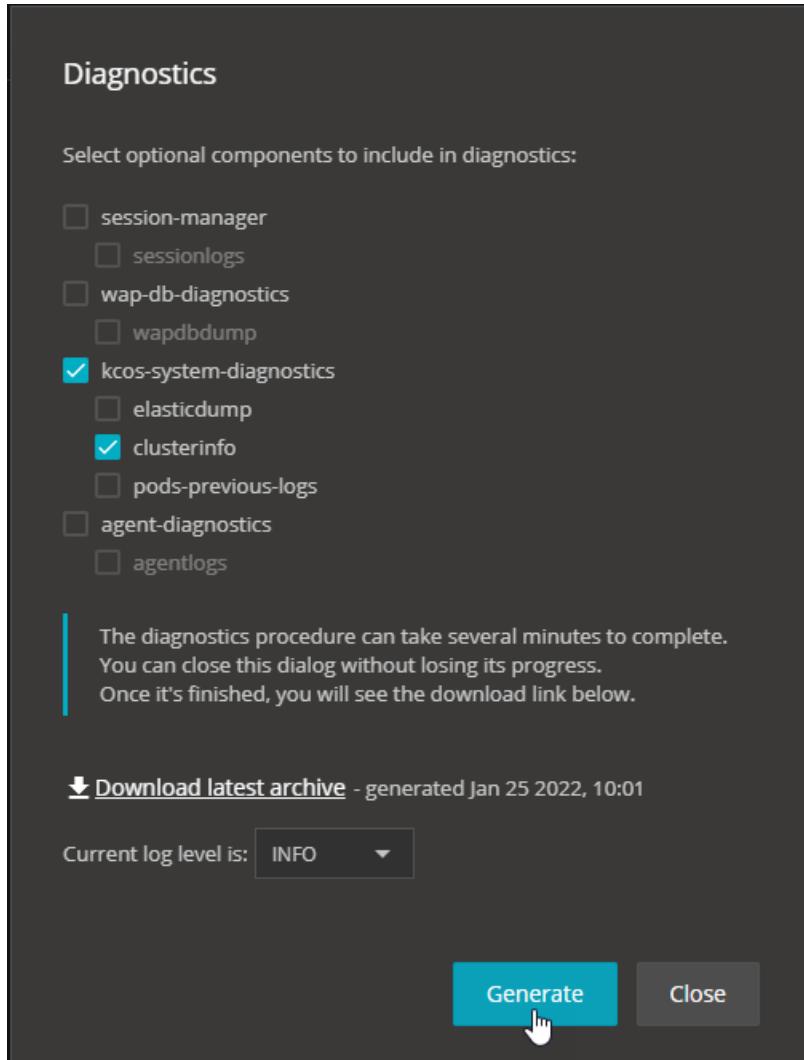
Collect Diagnostics

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

To collect diagnostics, do the following:

1. Select the wheel icon > **Collect Diagnostics**. The Diagnostics window appears.
2. If needed, select the optional components to include in the diagnostics report.
3. Select the log level used to collect diagnostics. Available options are:
 - **Error**
 - **Warn**
 - **Info**
 - **Debug**
4. Select **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.

For example ...



Change Dashboard theme

By default, the LoadCore Dashboard theme is set to Dark theme.

To change the dashboard theme, do the following:

1. Select the wheel icon on the top right corner of the Dashboard page. The general settings menu appears.
2. From the general settings menu, select **Themes**. The following options are available:
 - **Light**
 - **Dark**
 - **Caranu Light**
 - **Caranu Dark**
3. Select the desired theme.

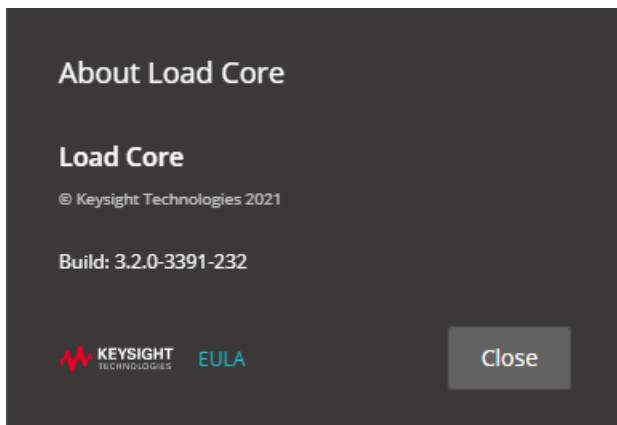
Help

After you have logged in, you can revisit and accept the Keysight Software End User License Agreement, by selecting **EULA**.

Select **About** to display details regarding the LoadCore software version.

You can also access your REST API Key. The key can be copied (select **Copy Key**) and re-used for further purposes.

For example ...



Log out

To log out of the LoadCore browser-based Web UI, select the Settings menu from the upper-right corner of the Dashboard page and select **Logout**. You will be redirected to the log in page.

Configure LoadCore with LDAP/AD

This section describes the steps needed in order to configure LoadCore with LDAP/AD:

1. Select the wheel icon > **Administration** > **Access Control**.

The screenshot shows the LoadCore Administration interface. In the top right, there is a user icon with a blue notification badge (2) and the word "admin". A sidebar on the right has a "dropdown arrow" icon. The main menu items are "Agent Management", "Access Control" (which is highlighted in yellow), "Software Updates", and "-----". To the right of the menu, there are links for "Administration", "Application Settings", "Collect Diagnostics", "Rest API Browser", "Themes", "Help", and "Logout".

A separate browser page opens displaying all access control settings.

2. Add a default group. Default groups allow you to automatically assign group membership to users.

First, you need to create a new group and set up the default group's role for assigned every Active Directory's user role.

Then, to make it as a default group:

3. Add a provider.

To perform these actions you must be logged in as a realm administrator or super user. You will need access to the server logs. You may require help from your companies AD team.

To begin configuring a LDAP identity provider, go to User Federation and select **LDAP** from the drop down list.

The LDAP settings should look like the following:

- **Vendor** - The most important setting is the Vendor drop down, which will fill the page with default values for different LDAP providers. Options include **Active Directory**, **Red Hat Directory Server**, **Tivoli**, **Novell eDirectory** and **Others**. You may need to ask your LDAP administrator.
- **Edit Mode** - Edit Mode must be set to **UNSYNCED** for the Terms & Conditions acceptance to work.
- **Username LDAP attribute** - Name of the LDAP attribute that will be mapped to the Keycloak username. Active Directory installations may use **cn** or **sAMAccountName**. Others often use **uid**.
- **RDN LDAP attribute** - Name of the LDAP attribute that will be used as the RDN for a typical user DN lookup. This is often the same as the above **Username LDAP attribute**, but does not have to be. For example, Active Directory installations may use **cn** for this attribute while using **sAMAccountName** for the Username LDAP attribute.
- **UUID LDAP attribute** - Name of an LDAP attribute that will be unique to all users in the tree. For example, Active Directory installations should use **objectGUID**. Other LDAP vendors typically define a UUID attribute, but if your implementation does not have one, any other unique attribute (such as **uid** or **entryDN**) may be used.
- **User Object Classes** - Values of the LDAP objectClass attributes for users, separated by a comma. This is used in the search term for looking up existing LDAP users, and if read-write sync is enabled, new users will be added to LDAP with these objectClass values as well.
- **Connection Url** - This will have been provided by the AD contact. Note that "l" in the middle is an "el", as in "ldap".
- **Users DN** - Example: cn=users:dc=ad,dc=keysight,dc=com
- **Custom User LDAP filter** - format : (logic (condition 1) (condition 2) ... (condition n))

Logic	Symbol
AND	&
OR	
NOT	!

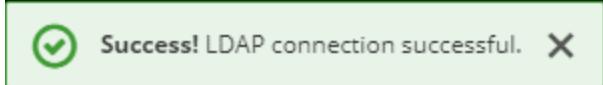
For Example:

(&(objectclass=user) (objectcategory=person) (! (UserAccountControl:1.2.840.113556.1.4.803:=2))) means "User AND Person AND Not Account Disabled"

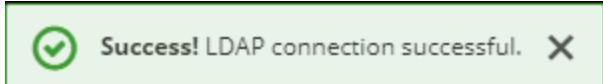
It reduced Users number from 26185 to 21262 in Keysight Active Directory on 10/12/2020.

Refer to [Active Directory User Related Searches](#) for more details.

- **Test Connection** - This button allows you to test if your connection to the LDAP server is correctly configured. After selecting the **Test connection** button, success is indicated by a success message on the top of the page.



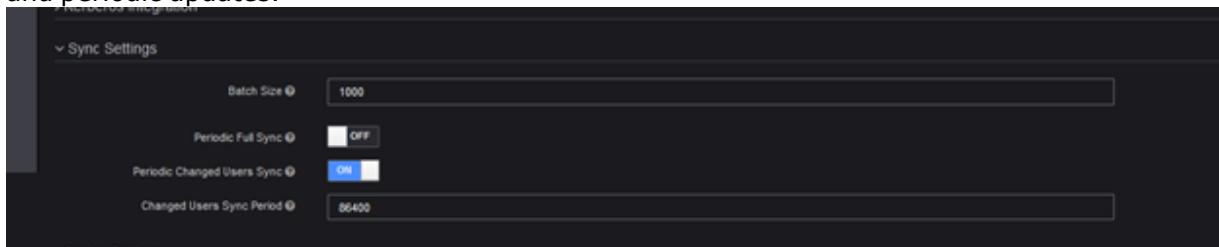
- **Test Authentication** - This button allows you to test if connection is correctly authenticated. After selecting the **Test Authentication** button success is indicated by a success message on the top of the page.



IMPORTANT Make sure that Edit Mode is set to **UNSYNCED**. Without this, new users will get an error and not be able to log in when they accept the EULA.

4. Configure synchronization settings.

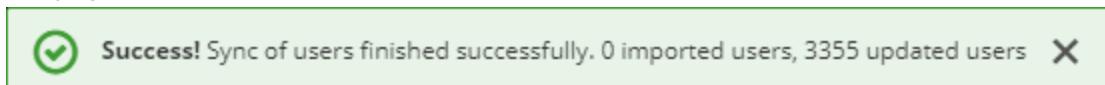
If you have a large number of users to import, it can be helpful to set up batch synchronization and periodic updates.



5. Configure LDAP mapper.

After saving the initial configuration, you can add extra user information (country, department, state and title).

6. Select the **Synchronize all users** button. The success message will be displayed on the top of the page.



IMPORTANT

It takes a long time to do a full synchronization. Wait until the success or failed message is displayed.

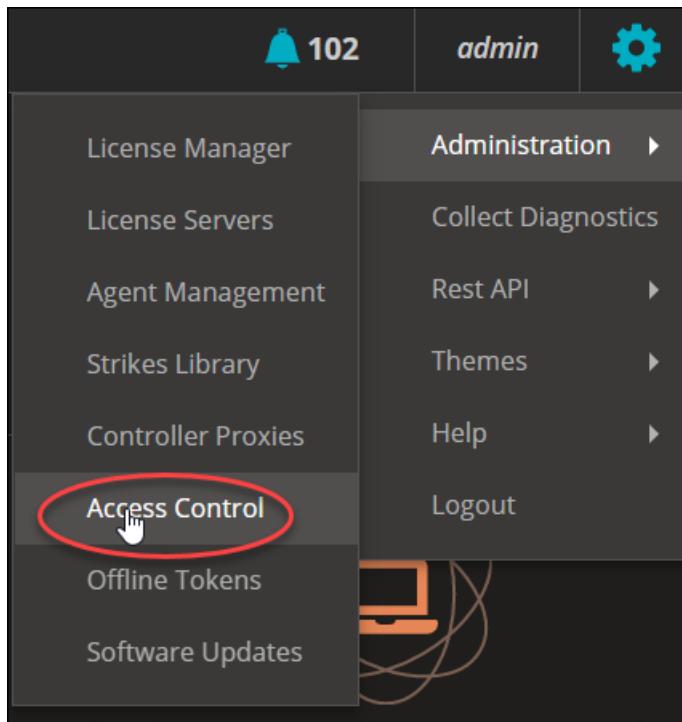
Reset Password for Regular Users

This section describes the steps needed in order to reset the LoadCore log in password for regular users.

IMPORTANT

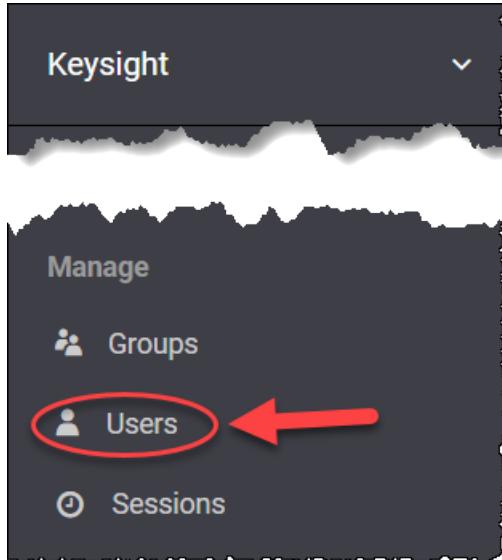
The password can be changed only by an **ADMIN** user.

1. Select the wheel icon > **Administration** > **Access Control**.



A separate browser page opens, displaying all access control settings.

2. From the Manage section, select **Users**.



The Users section is displayed.

- From the Lookup tab, use the search function to find a specific user or select **View all users** to display all users and, then, select it from the list.

A screenshot of a table titled "Users". The table has columns: ID, Username, Email, Last Name, First Name, and Actions. There are two rows:

ID	Username	Email	Last Name	First Name	Actions
2527e098-9acd-48a9-8ab...	admin	admin@example.org	Admin	Default	Edit Delete
1a0287b9-9345-4858-b7b...	tester				Edit Delete

Select the **Edit** action for the user that needs a password reset. The user's profile section is displayed.

- Select **Credentials**.

A screenshot of a user profile page for "Tester". The top navigation bar shows "Users > tester". Below it is a "Details" card with "Tester" and a trash icon. A navigation bar below the card includes tabs: Details, Attributes, Credentials (which is highlighted with a red oval and has a red arrow pointing to it), Role Mappings, Groups, Consents, and Sessions. The "Details" card contains:

ID	1a0287b9-9345-4858-b7b6-f49d245a3a61
Created At	4/18/22 12:59:58 PM
Username	tester

- Set the new password and select **Set Password** in order to apply the changes.

Users > tester

Tester !

Details Attributes **Credentials** Role Mappings Groups Consents Sessions

Manage Credentials

Position	Type	User Label	Data
Set Password			
Password	*****		<input type="button" value="eye"/>
Password Confirmation	*****		<input type="button" value="eye"/>
Temporary <small>?</small>	<input checked="" type="checkbox"/> ON		
<input style="outline: none; border: 1px solid red; border-radius: 5px; padding: 5px; width: 100%; height: 30px; font-size: 1em; font-weight: bold; color: black; background-color: transparent;" type="button" value="Set Password"/>			

CHAPTER 4

License Manager

This section displays details regarding the current situation of your LoadCore licenses.

The screenshot shows the LoadCore License Manager interface. At the top, there is a header bar with the LoadCore logo, a bell icon with '1' notification, the user 'admin', and a gear icon. Below the header is a table with columns: Part ID, Product, Description, License Expiration, Maintenance Expiration, Activation Code, Quantity, and Manage Reservation. Underneath the table are several buttons: 'Activate Licenses', 'Sync Licenses', 'Offline Operations', 'License Statistics', and 'Deactivate Licenses'.

The following options are displayed on the Licensing section:

- **Activate licenses** - select this in order to activate LoadCore licenses using Activation Codes.

The screenshot shows the 'Activate Licenses' dialog box. It has a section for 'Enter License Data:' with an example of license codes and a 'Load Data' button. Below this is a section for 'Select and edit activation codes:' with a table and two buttons at the bottom: 'Activate' and 'Close'.

Product	Description	Activation Code	Entitlement Code	Total	Available	To Activate

- **Sync licenses** - select this in order to synchronize LoadCore licenses.
- **Offline operations** - select this in order to perform licensing operation when you do not have internet connectivity.

Keysight Licensing Offline Operations

It seems that you don't have internet connectivity. You may be offline or your proxy or firewall settings might have blocked the access to the Keysight Software Manager Web Server.

In order to perform your licensing operation you will have to follow the steps below:

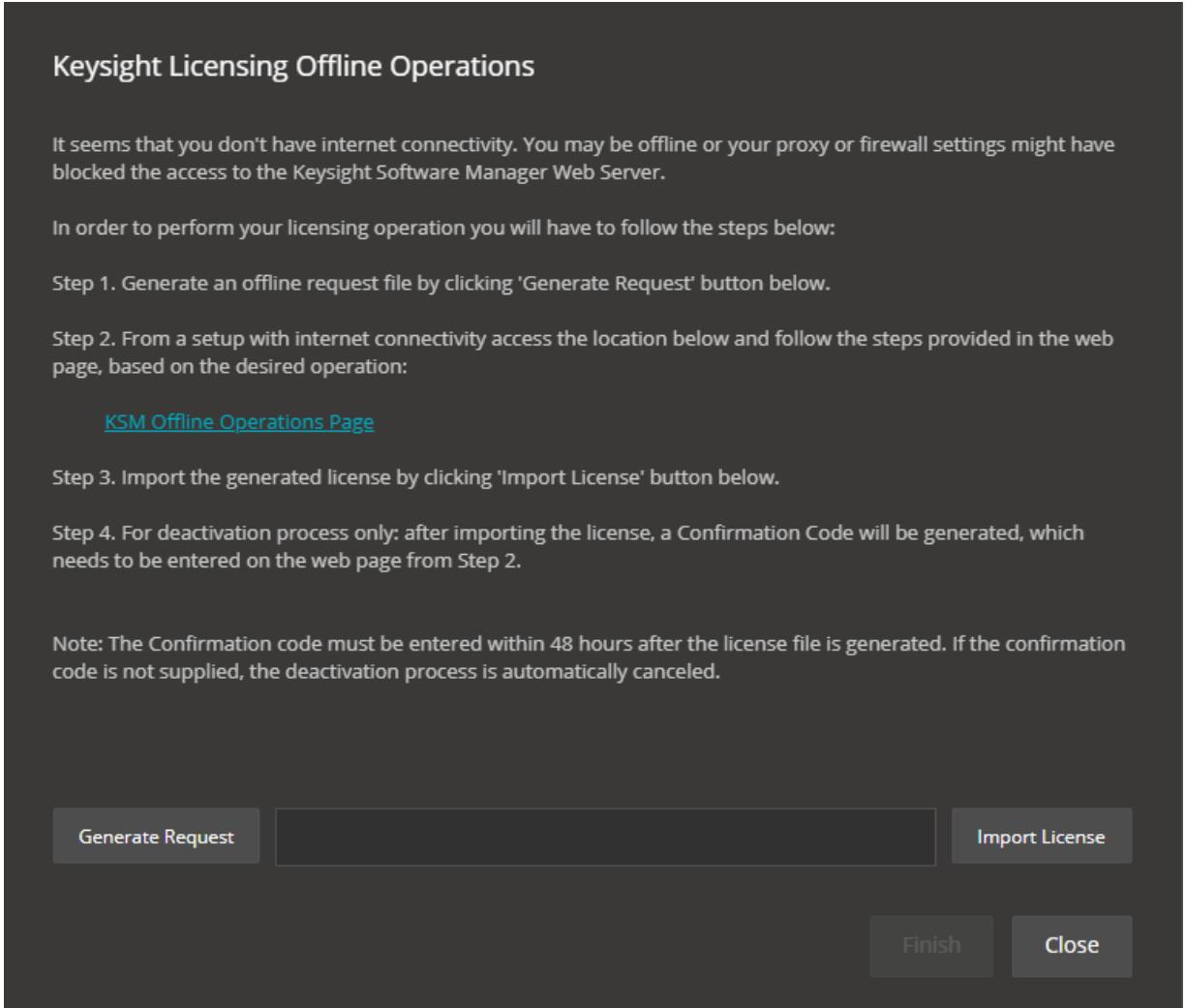
Step 1. Generate an offline request file by clicking 'Generate Request' button below.

Step 2. From a setup with internet connectivity access the location below and follow the steps provided in the web page, based on the desired operation:
[KSM Offline Operations Page](#)

Step 3. Import the generated license by clicking 'Import License' button below.

Step 4. For deactivation process only: after importing the license, a Confirmation Code will be generated, which needs to be entered on the web page from Step 2.

Note: The Confirmation code must be entered within 48 hours after the license file is generated. If the confirmation code is not supplied, the deactivation process is automatically canceled.



- **License statistics** - select this to display metrics about your LoadCore licenses.
 - **Deactivate licenses** - use this option in order to deactivate LoadCore licenses.
- NOTE** It is recommended to deactivate the license before deleting a LoadCore VM. This way you can easily reuse the same license (Activation Code) when deploying another LoadCore VM.

CHAPTER 5

Traffic agents assignment and management

Agent(s) Assignment

The traffic agents generate traffic for both user plane and control plane.

IMPORTANT You can create and save your test scenario in the LoadCore web UI, but you cannot run it before assigning traffic agent to the nodes.

To assign traffic agents to one of your LoadCore nodes, you have to select the traffic agent icon on the top right corner of the of the LoadCore node:

The traffic agent icon can be displayed as follows:

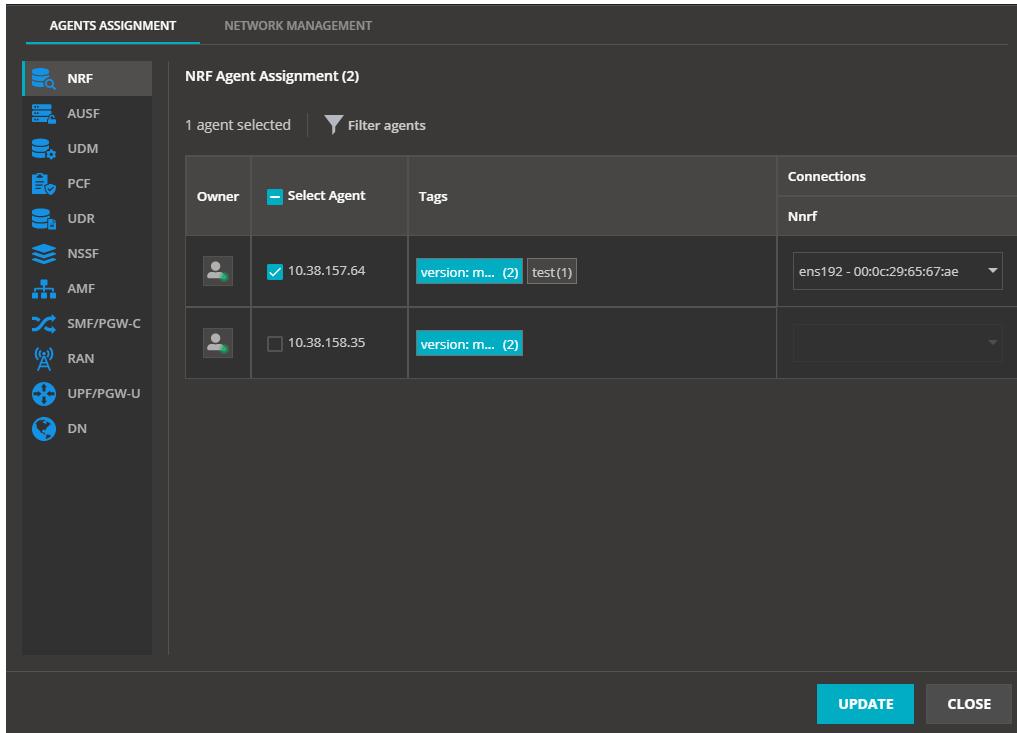
- a.  - no traffic agent(s) selected for this node, or
- b.  - traffic agent(s) have been selected for this node;

NOTE There is an another state of this traffic agents icon. This state is displayed as red icon and appears when loading a configuration from disk that has agents assigned to the a node, but that agent is not reachable, or no longer exists.

TIP When hovering over the traffic agent icon, a message is displayed showing the number of traffic agents enabled for that LoadCore node.

When you select the agent icon, the Agents Assignment window is opened. From here, you can assign one or more agents to your current LoadCore node or, you can choose to assign the agents to different nodes based on your test configuration.

For example ...



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

Column	Description
Owner	Indicates the agent's owner.
Select Agent	<p>Allows you to select one or more agents from the available ones.</p> <p>To select a specific agent, select the check-box associated to the agent's IP address. When hovering over the IP address of an agent, the agent ID is displayed.</p> <p>To select all available agents, select the Select Agent check-box.</p>
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 ones) - more details are displayed when hovering over the system tag icon. user tags (gray ones) - these tags can be added by users from the Agent Management window. <p>Each tag indicates the number of agents to which it was associated.</p>
Connections	<p>For each wireless connection, it displays the available interface and the MAC address. The interface can be selected from the drop-down list.</p> <p>NOTE For the LoadCore nodes that have multiple interfaces (for example, the AMF node), for each interface, you can change the interface type using the drill-down option.</p>

From the left side of the Agents Assignment window, you can select another node from the list and start configure the agents for that node also. This way, you can configure agents for all the nodes necessary for your test configuration.

All selected agents are displayed on the Network Management window.

For example ...

The screenshot shows the Network Management window with three agents selected. The agents are listed in a table:

Order	Agent	Tags	Impairment Profile	Agent Interface		Network Stack	SRIOV	Traffic Capture	Entity
				Name	MAC				
1	10.38.156.240	txStack: OFF(3) build: 490(2)	None	ens192	00:0c:29:c4:f2:a2	Linux Stack	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AMF
2	10.38.157.199	txStack: OFF(3) build: 3591(1)	None	ens192	00:0c:29:2af7:39	Linux Stack	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AMF
3	10.38.156.153	txStack: OFF(3) build: 490(2)	None	ens192	00:0c:29:6f:5b:0d	Linux Stack	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AMF

At the bottom right of the window are two buttons: "UPDATE" and "CLOSE".

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

Column	Description
Order	Allows you to select the agent distribution order when running with multiple agents on the same node (and you do not want to use a switch to connect all agents).
Agent	Displays the agent's IP address. When hovering over the IP address of the agent, the agent ID is displayed.
Tags	<p>This column displays the tags associated to each agent.</p> <p>There are two types of tags:</p> <ul style="list-style-type: none"> system tags (blue ones) - more details are displayed when hovering over the system tag icon. user tags (gray ones) - these tags can be added by users from the Agent Management window. <p>Each tag indicates the number of agents to which it was associated.</p>
Impairment profile	Allows you to select an impairment profile from the drop-down list.

Column	Description
Agent Interface	Displays details regarding the agent's interface name and MAC address.
Network Stack	<p>NOTE This setting is not available for the Wireless SBA test.</p> <p>Allows you to select the network stack used to run the test. Available options:</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 (this is displayed on the Tags column).</p>
SRIoV	<p>NOTE This setting is not available for the Wireless SBA test.</p> <p>This option is disabled when Network Stack is set to Linux Stack. For IxStack over Raw Sockets or IxStack over DPDK, this option is enabled based on the selection (it can be enabled/disabled based on your agents configuration).</p>
Traffic Capture	Allows you to enable traffic capture on all interfaces or just on specific ones, based on your test configuration.
Entity	Displays the nodes on which the agent has been assigned. When hovering over the node, it displays the interfaces also.

IMPORTANT To run tests using IxStack over Raw Sockets or IxStack over DPDK you need at least 2 agents.

For example ...

AGENTS ASSIGNMENT		NETWORK MANAGEMENT					
2 agents selected		<input type="button" value="Filter agents"/>					
Order	Agent	Tags	Impairment Profile				
Name	MAC	Network Stack	SRIoV	Traffic Capture	Entity		
1	10.38.157.185	IxStack: ON (2) DDPK (2) build: 3525 (2)	None	ens192 00:0c:29:ab:ac:b5 Linux Stack	<input checked="" type="checkbox"/>	<input type="checkbox"/>	NRF AUSF UDM PCF UDR AMF SMF/PGW-C UPF/PGW-U DN
				ens160 00:0c:29:ab:ac:ab IxStack over Raw Sockets	<input checked="" type="checkbox"/>	<input type="checkbox"/>	UPF/PGW-U
2	10.38.157.47	IxStack: ON (2) DDPK (2) build: 3525 (2)	None	ens192 00:0c:29:40:42:dd IxStack over Raw Sockets	<input checked="" type="checkbox"/>	<input type="checkbox"/>	RAN

The first agent is configured on the RAN and the second one on the UPF/PGW-U. The second agent has two interfaces, one on the UPF N3 interface that connects with RAN and the second one to connect with the rest of the topology. This is done because an agent can not have 2 IxStack interfaces.

On both windows, you can filter the available agents by tag names. To do this, select **Filter agents**, type the name of the tag or select it from the available list and select **Close**. The content on the

Agents Assignment/Network Management window is updated with the filtering results. To remove the filtering results, select **Clear**.

To apply the changes done on the Agents Assignment window and Network Management, select **Update**.

Agent(s) Management

To open the Agent Management window, select Gear menu > **Administration > Agent Management**.

For example ...

Agent IP	Owner	Status	Tags	Test NICs	Hostname	Memory	CPU info			
							Model	Frequency	Cores	
<input checked="" type="checkbox"/> 10.38.157.64			Stopped	version: m... (2) test(1)	ens192 ens160	5GCTE-27085763a	4 GB	Intel®	3.1 GHz	4
<input type="checkbox"/> 10.38.158.35			Stopped	version: m... (2)	ens192 ens160	5GCTE-27085763a	4 GB	Intel®	3.1 GHz	4

Buttons at the bottom: CLEAR OWNERSHIP, HARD REBOOT, DELETE.

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

Column	Description
Agent IP	Allows you to select one or more agents from the available ones. To select a specific agent, select the check-box associated to the agent's IP address. When hovering over the IP address of an agent, the agent ID is displayed. To select all available agents, select the Agent IP check-box.
Owner	Indicates the agent's owner.
Status	Indicates the current status of the agent.
Tags	This column displays the tags associated to each agent. There are two types of tags:

Column	Description
	<ul style="list-style-type: none"> • system tags (blue ones) - more details are displayed when hovering over the system tag icon. • user tags (gray ones) - users can add/remove custom tags, more details here. <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 also.
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.

You can filter the available agents by tag names. To do this, select **Filter agents**, type the name of the tag or select it from the available list and select **Close**. The content on the Agent Management window is updated with the filtering results. To remove the filtering results, select **Clear**.

To search for agents, use the search bar on the upper-right corner of the Agent Management window.

You can add custom tag names to agents, as follows:

1. Select one or more agents from the ones available.
2. Select **Tag as**.
3. Type the name of the tag in the **Search or add tag** field and select **Add**. Select **Update** to add the tag name.

To remove a tag name, do the following:

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

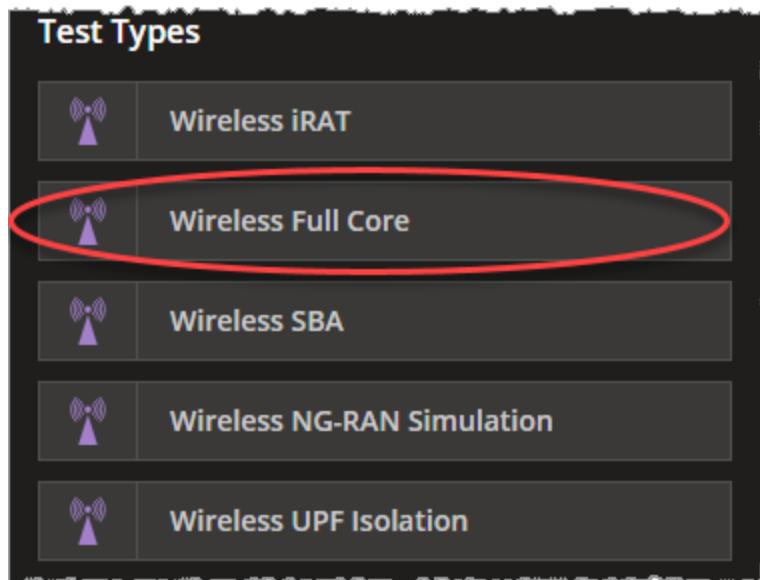
When you select one or more agents, the following actions became available:

- **Clear Ownership** - Releases your ownership of the selected agent(s).
- **Hard Reboot** - performs a hard reboot on the agent(s).
- **Delete** - removes the selected agent(s) from the Agent Management list.

CHAPTER 6

Full Core tests: configuration settings

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



In a Full Core test, the entire test topology is available for configuration to enable your test requirements. There is no pre-established DUT: you can designate any of the topology nodes as device under test. You can enable and disable the simulated nodes as needed to customize your test configuration.

Topics:

Global Settings	78
Global Settings panel	80
DNS Settings	80
Advanced Settings	81
DNNs panel	85
DNN configuration settings	86
Session AMBR configuration settings	89
ePCO configuration settings	90

Traffic Control Settings configuration	90
Impairment	91
QoS Flows panel	92
QoS Flow configuration settings	93
QoS Flow Packet Filter configuration settings	96
QoS Flow Max Packet Loss Rate settings	97
QoS Flow ARP configuration settings	97
QoS Flow MBR configuration settings	98
QoS Flow GBR configuration settings	98
AUSF configuration settings	99
AUSF Ranges panel	100
AUSF Range panel	100
AUSF node settings	101
AUSF Nausf interface settings	102
AUSF Remote SBA Nodes	103
AMF configuration settings	105
AMF Ranges panel	106
AMF Range settings	107
AMF node settings	108
AMF N2 interface settings	111
AMF Namf interface settings	112
AMF N26 Interface Settings	112
AMF remote SBA nodes	113
DN configuration settings	118
DN Ranges panel	119
DN Range panel	119
DN N6 interface settings	120
DN UE routes settings	121
DN User Plane	121
DN Application Traffic Generator	122
DN Stateless UDP Traffic Generator	129
MME configuration settings	131

MME Ranges panel	132
MME Range panel	132
MME node settings	134
MME S11 Interface Settings	135
MME N26 Interface Settings	136
MME S1 Interface Settings	137
MME S6a Interface Settings	139
MME Diameter	140
NRF configuration settings	141
NRF Ranges panel	142
NRF Range panel	142
NRF node settings	143
NRF Nnrf interface settings	144
SCP configuration settings	144
SCP Ranges panel	145
SCP Range panel	145
SCP interface settings	146
SCP Remote SBA Nodes	147
NSSF configuration settings	149
NSSF Ranges panel	150
NSSF Range panel	150
NSSF node settings	151
Nnssf Interface Settings	152
Remote SBA nodes	153
NSSF Restricted NSSAIs	154
NSSF Network Slices	155
NSSF Configured NSSAI	156
PCF/PCRF configuration settings	157
PCF Ranges panel	158
PCF Range panel	159
PCF node settings	160
PCRF node settings	161

PCF service area restrictions	161
PCF Npcf interface settings	162
PCRF Rx interface settings	163
PCF remote SBA nodes	164
RAN configuration settings	166
gNodeB	167
gNodeB Ranges panel	168
gNodeB Range settings	172
gNodeB node settings	173
gNodeB NSSAI settings	174
gNodeB N2 interface settings	175
gNodeB N3 interface settings	177
eNodeB	179
eNodeB Ranges panel	180
eNodeB Range Settings	180
eNodeB Node Settings	181
S1 Interface Settings	182
S1-U Interface Settings	183
Passthrough interface settings	185
SGW configuration settings	187
SGW Ranges panel	188
SGW Range panel	188
SGW S1-U Interface Settings	190
SGW S5-C Interface Settings	191
SGW S5-U Interface Settings	192
SGW S11 Interface Settings	193
SGW DUT S11 Interface Settings	194
SMF/PGW-C configuration settings	195
SMF/PGW-C Ranges panel	196
SMF/PGW-C Range settings	197
SMF node settings	198
SMF N4 interface settings	199

SMF Nsmf interface settings	200
SMF remote SBA nodes	201
NEF configuration settings	204
NEF Ranges panel	204
NEF Range panel	205
NEF Nnef interface settings	206
NEF Remote SBA Nodes	206
UDM/HSS configuration settings	209
UDM/HSS Ranges panel	210
UDM/HSS Range panel	211
UDM/HSS node settings	211
UDM/HSS Nudm interface settings	215
UDM/HSS Remote SBA Nodes	216
UDR configuration settings	218
UDR Ranges panel	218
UDR Range panel	218
UDR Nudr interface settings	219
UDR Remote SBA Nodes	220
IMS configuration settings	221
CSCF Range panel	221
CSCF N6 interface settings	222
CSCF Rx interface settings	223
CSCF UE routes settings	224
CSCF remote SBA nodes	224
Media Function Range panel	225
UPF/PGW-U configuration settings	226
UPF/PGW-U Ranges panel	227
UPF/PGW-U Range panel	227
UPF N3 interface settings	228
UPF N4 interface settings	229
UPF N6 interface settings	231
UPF N9 interface settings	231

SMSF configuration settings	234
SMSF Ranges panel	234
SMSF Range panel	235
SMSF node settings	235
SMSF Nsmsf interface settings	236
SMSF Remote SBA Nodes	237
5G-EIR configuration settings	238
5G-EIR Ranges panel	238
5G-EIR Range panel	238
5G-EIR node settings	239
5G-EIR N5g-eir interface settings	239
5G-EIR Remote SBA Nodes	240
UE configuration settings	242
UE Ranges panel	243
UE Range panel	244
Range Settings	246
UE Identification settings	247
UE Security settings	247
UE Settings settings	249
UE Shared Data IDs	253
UE Subscribed AMBR settings	253
Service Area Restriction settings	253
Forbidden Areas	255
DNNs Config	256
Notifications	257
SMS Configuration	258
Equipment Status	259
Network Slicing settings	260
UE NSSAI settings	261
UDM Default NSSAI settings	262
UDM SNSSAI Mappings	262
UDR SNSSAI Settings	263

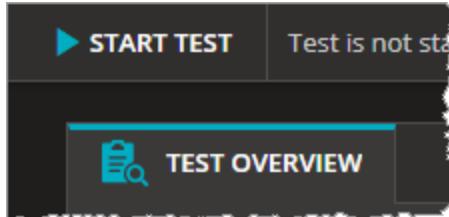
Objectives	264
Control Plane Objective	265
About primary objectives	266
Primary Control Plane Objective	268
Secondary Control Plane Objective	270
User Plane Objectives	279
Stateless UDP Traffic	280
Data Traffic	281
Voice Traffic	284
Video OTT Traffic	287
DNS Client Traffic	290
Predefined Applications Traffic	293
NF Discovery service	304

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:

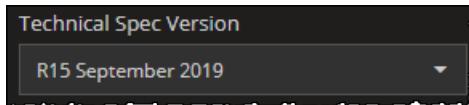


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



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

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

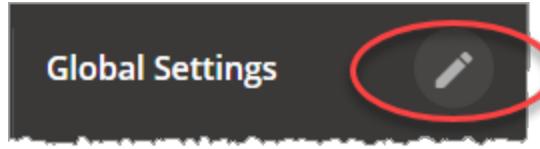


- Access and configure the following settings:

Global Settings panel	80
DNS Settings	80
Advanced Settings	81
DNNs panel	85
DNN configuration settings	86
Session AMBR configuration settings	89
ePCO configuration settings	90
Traffic Control Settings configuration	90
Impairment	91
QoS Flows panel	92
QoS Flow configuration settings	93
QoS Flow Packet Filter configuration settings	96
QoS Flow Max Packet Loss Rate settings	97

QoS Flow ARP configuration settings	97
QoS Flow MBR configuration settings	98
QoS Flow GBR configuration settings	98

Global Settings panel



When you open the Global Settings for editing (from the **Test Overview** section), LoadCore 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. These include settings with which you control the Stream Control Transmission Protocol (SCTP) connection rates between NG-RAN and AMF, a selection option for the Network Instance form, and selects for more detailed settings. (SCTP—which operates in the transport layer of the NG-C signaling bearer—provides for the reliable transport of signaling messages.)

Setting	Description
Node Start Rate	Set the desired start rate for SCTP connections between the NG-RAN and the AMF (connections per second).
Node Stop Rate	Set the desired stop rate for SCTP connections between the NG-RAN and the AMF (connections per second).
Network Instance Format	Select the encoding format for the network instance: string or label-list.
<i>Links to detailed settings:</i>	
DNS Settings	DNS Settings below
Advanced Settings	Advanced Settings on the facing page
DNNs	DNNs panel on page 85
Impairment	Impairment on page 91
QoS Flows	QoS Flows panel on page 92

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.

Setting	Description
<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
Ignore Offline Agents At Runtime	When this option is selected, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.
Overwrite Capture Size for IxStack	Select this check box 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 check box to enable it.
Enable Capture On Loopback Interface	Select this check box to enable packet capture on the loopback interface.
Enable Per UE Stats	Select this check box to enable per UE statistics.
Enable Control Plane Advanced Stats	Select this check box to enable control plane latency statistics.
Enable User Plane Advanced	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.

Setting	Description
Stats	<ul style="list-style-type: none"> • 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	Selected by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval (sec)	<p>This option becomes available only when Automated Polling Interval check-box is unselected.</p> <p>It allows you to create a custom polling interval.</p>
Log Level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful to debug the application.
Log Tags	<p>Select one or more tags from the drop-down list.</p> <p>Log Tags are used to collect specific information in the logs; they work with Debug and with Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.</p>

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	DESCRIPTION IS NOT YET AVAILABLE.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select the check box to enable this option.
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	

Setting	Description
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.

Response Cache

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

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

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

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

Control Plane Latency Statistics

There are two types of control plane latency statistics available:

- Control Plane HTTP Latency Statistics
- Control Plane Procedure Latency Statistics

For HTTP, the control plane latency statistics are measured per HTTP transaction. For the control plane HTTP latency statistics, on the client side, the latency measures the time between the moment when the request is sent and the moment when the answer is received. On the server side, the latency measures the time between the moment when the request is received and the moment when the answer is sent.

For NGAP, NAS and PFCP, the control plane latency statistics are measured per procedure. In this case, the control plane procedure latency value represents the time between the moment when the first message in the procedure is sent or received and the moment when the last message in the procedure is sent or received.

IMPORTANT

The time shown in statistics may be slightly different than the time computed in any capturing tool (for example, Wireshark) because of the time when the packets are actually captured.

Latency buckets:

- 0us - 125us
- 125us - 250us
- 250us - 500us
- 500us - 1ms
- 1ms - 5ms
- 5ms - 10ms
- 10ms - 15ms
- 15ms - 20ms
- 20ms - inf

NOTE

If enabled, the control plane latency statistics will not be displayed in predefined dashboards in LoadCore statistics user interface. To display these statistics you will need to use custom dashboards.

Retrieve captured packets

After enabling packet capture, and running the test, to download the generated packet captures, you need to use a SFTP client (for example, WinSCP) to retrieve the captures from `/opt/5gc-test-engine` on each of the agents.

The packet capture can be identified as follows:

- `latestCapture.pcap`, when running the test without DPDK activated.
- `latestIxStackCapture.pcap` when running the test with DPDK activated.

DNNs panel

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

When setting up a LoadCore test, these DNN configurations become immediately available for selection in the UDM and UE configurations.

Accessing the configuration settings

To access the DNN configuration settings, select **DNNs** from the the **Global Settings** panel. LoadCore 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	86
Session AMBR configuration settings	89
ePCO configuration settings	90
Traffic Control Settings configuration	90

DNN configuration settings

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

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

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

Setting	Description
<i>DNN:</i>	
DNN	<p>Enter the DNN value for this DNN definition. For example: <code>dnn.keysight.com</code>.</p> <p>A DNN (as is the case with an EPS APN) is composed of two parts:</p> <ul style="list-style-type: none"> • A mandatory Network Identifier that defines the external network to which the UPF is connected. • An optional Operator Identifier that defines the PLMN backbone in which the UPF is located. <p>A 5GS Data Network Name (DNN) is equivalent to an EPS APN. It is a reference to a data network, and it may be used to select an SMF or UPF for a PDU session and to determine policies applicable to the PDU session.</p> <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> <p>NOTE The start_value and end_value must have the same length. For example, we can configure <code>dnn[008-999,1]</code> and obtain <code>dnn008,dnn009,...,dnn998,dnn999</code>. Syntaxes <code>dnn[8-999,1]</code> or <code>[008-1000,1]</code> are not valid as the start and end value lengths are different.</p> <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>

Setting	Description
	<p>IMPORTANT If multiple sequence generators are configured and their pools overlap (for example: dnn[000-600,1].keysight.com dnn[500-999,1].keysight.com), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the start_value (they might start with an intermediate value in the second pool).</p>
PDU Type	Select the desired PDU type: IPv4, IPv6, IPv4v6 or Ethernet.
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 on page 93.</p>
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.
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	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.
Subscription	Select the desired Subscription Category for this range of UEs.

Setting	Description
Categories	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).
Guaranteed Bit Rate Uplink	The guaranteed bit rate (bps) for uplink traffic. This is the uplink bit rate that the QoS Flow associated with this DNN is expected to provide.
Guaranteed Bit Rate Downlink	The guaranteed bit rate (bps) for downlink traffic. This is the downlink bit rate that the QoS Flow associated with this DNN is expected to provide.
EPS Interworking	Select this option if the UE subscription data indicates support for interworking with EPS for this DNN.
Is Local Area DN	Select this option if connectivity with the DNN is provided through a Local Area Data Network (LADN). A Local Area Data Network is a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.
ADC Support	Select this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.
Subscriber Spending Limits	Select this option if the DNN will support PDU session policies that are based on subscriber spending limits.
Offline	Select this option if the DNN will support the offline charging method for PDUs sessions.
Online	Select this option if the DNN will support the online charging method for PDUs sessions.
Is Emergency DNN	When this option is selected, if an UE range has mapped this type of DNN, it will perform an emergency PDU Session.
IPv4 Index	The IPv4 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv4 addresses.
IPv6 Index	The IPv6 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv6 addresses.
MPS Priority	Select this option if the DNN will support subscription to MPS priority service. The priority applies to all traffic on the PDU Session.
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.

Setting	Description
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.
PGW	Select an PGW range from the drop-down list. All of the SGW ranges that you have enabled for the test are available for selection. If your test configuration does not require a PGW connection for the selected DNN, then select <i>None</i> .
Session Rule Name	Set the session rule name.
GBR	<i>Select this option to open the GBR panel.</i>
Guaranteed Bit Rate Uplink	Specify the guaranteed bit rate for the uplink traffic.
Guaranteed Bit Rate Downlink	Specify the guaranteed bit rate for the downlink traffic.
Session AMBR	<i>Select this option to open a new panel that contains the Session AMBR settings. These settings are described in Session AMBR configuration settings below.</i>
ePCO	<i>Select this option to open the extended protocol configuration options panel. These settings are described in ePCO configuration settings on the next page.</i>
Traffic Control Settings	<i>Select this option to open the traffic control settings panel. These settings are described in Traffic Control Settings configuration on the next page.</i>

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 LoadCore DNN configuration has its own unique configuration settings, which include:

- The main DNN settings, described in [DNN configuration settings on page 86](#).
- The DNN's Session AMBR settings, described below.

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

The ePCO option was added to LoadCore, on the NG-RAN side, in order to avoid errors when inter operating with a DUT AMF.

The option refers to sending ePCO IE (extended Protocol Configuration Options IE) in PDU Session Establishment Request message, containing DNS Server Address Request and/or MTU Size Request IEs.

The following tables describes the ePCO configuration settings.

Parameter	Description
Request DNS Server IP Address	Select the check box to enable this option.
Request IPv4 Link MTU	Select the check box to enable this option.

Known limitations:

- ePCO will only be sent from the NG-RAN, the feature is not supported on any other nodes.
- 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.

Parameter	Description
	Select the check box to enable it.
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.

f, 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.

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 LoadCore or overwrite it with your own value.

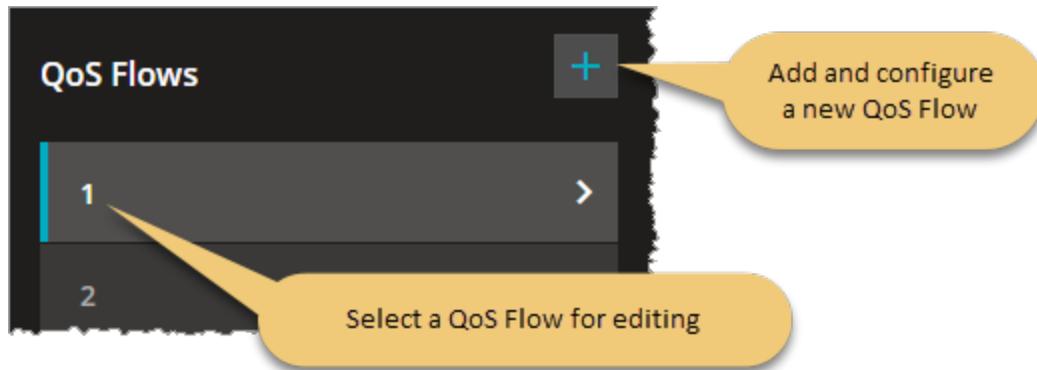
Setting	Description
Action Type	Select an option from the drop-down list: <ul style="list-style-type: none"> Custom script PFCP-drop message
Script file	This parameter is available only when Action Type is set to Custom script . It allows you to add a custom script, using the Upload button. To remove the script, select the Clear button.

QoS Flows panel

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

Accessing the configuration settings:

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



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

QoS Flow configuration settings	93
QoS Flow Packet Filter configuration settings	96
QoS Flow Max Packet Loss Rate settings	97
QoS Flow ARP configuration settings	97
QoS Flow MBR configuration settings	98
QoS Flow GBR configuration settings	98

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	Select this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow.
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 - LoadCore 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 - LoadCorePCF/PCRF needs information related to this flow/bearer from CSCF. • Video - LoadCorePCF/PCRF needs information related to this flow/bearer from CSCF.
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	Specify the 5QI value (decimal number). 5G QoS Identifier (5QI) is a scalar that is used as a reference to 5G QoS characteristics defined in TS 23.501, clause 5.7.4. These are access node-specific parameters that control QoS forwarding treatment for the QoS Flow (such as scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, among others). Standardized 5QI values have a one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in TS 23.501, table 5.7.4-1.
5QI Priority Level	Specify the 5QI Priority Level for this QoS Profile. 5QI Priority Level is a Policy Control parameter that accepts values from 1 through 127 (where 1 is the highest priority). It indicates a priority in scheduling resources among QoS Flows.
Resource	Select the type of resource that the QoS Flow requires: Guaranteed Bit Rate

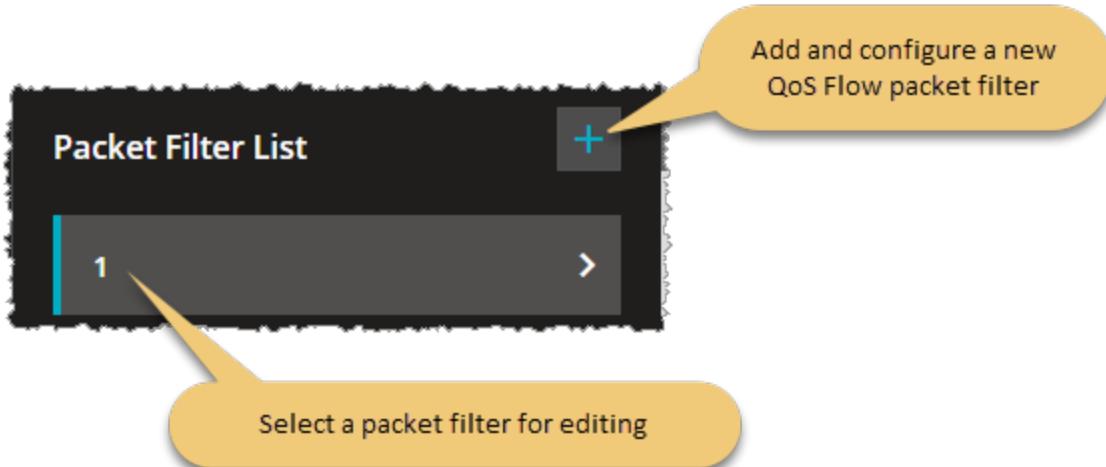
Setting	Description
Type	(GBR), Non-Guaranteed Bit Rate, or Delay Critical GBR. The Resource Type determines whether or not dedicated network resources related to a QoS Flow-level Guaranteed Flow Bit Rate (GFBR) value are permanently allocated to the flow.
Averaging Window	Specify the <i>Averaging window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

Setting	Description
Identifier	
PCC Rule Name	Set a value for this parameter.
Is Predefined Rule	Select the check box to enable this option.
Application Identifier	Set the application identifier value.
Send QoS Rule Precedence when Application identifier is configured	Select the check box to enable this option.
Move to Secondary Node in NSA topology	<p>Select the check box to enable this option.</p> <p>This option is part of the Option3x feature, for more details refer to UE Range Panel.</p>
Packet Filter List	<p>IMPORTANT This is available if Use Match-all Packet Filter option is not selected.</p> <p>Refer to the following topic for a description of the Packet Filter configuration settings: QoS Flow Packet Filter configuration settings on the next page.</p>
Max Packet Loss Rate	Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: QoS Flow Max Packet Loss Rate settings on page 97 .
ARP	Refer to the following topic for a description of the ARP configuration settings: QoS Flow ARP configuration settings on page 97 .
MBR	Refer to the following topic for a description of the MBR configuration settings: QoS Flow MBR configuration settings on page 98 .
GBR	Refer to the following topic for a description of the GBR configuration settings: QoS Flow GBR configuration settings on page 98 .

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.

Setting	Description
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	<p>Specify the ARP priority level.</p> <p>The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the</p>

Setting	Description
	home network and thus applicable when a UE is roaming.
Preemption Capability	Select this option if the packets in this QoS Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.
Preemption Vulnerability	Select this option if the packets in this QoS Flow are candidates for being preempted by other flows. When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.

QoS Flow MBR configuration settings

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

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

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

QoS Flow GBR configuration settings

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

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

Setting	Description
<i>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.

AUSF configuration settings



Authentication Server Function (AUSF) is the 5G core network service that handles authentication requests for 3GPP access and non-3GPP access networks. The AUSF serves as the termination point of user plane (UP) security, while providing the necessary authentication and authorization processes. It makes its services available to other network functions through the Nausf service-based interface. Multiple instances of AUSF may be deployed, with each instance storing specific data.

The configuration settings are described in the topics listed below.

Topics:

AUSF Ranges panel	100
AUSF Range panel	100
AUSF node settings	101
AUSF Nausf interface settings	102
AUSF Remote SBA Nodes	103

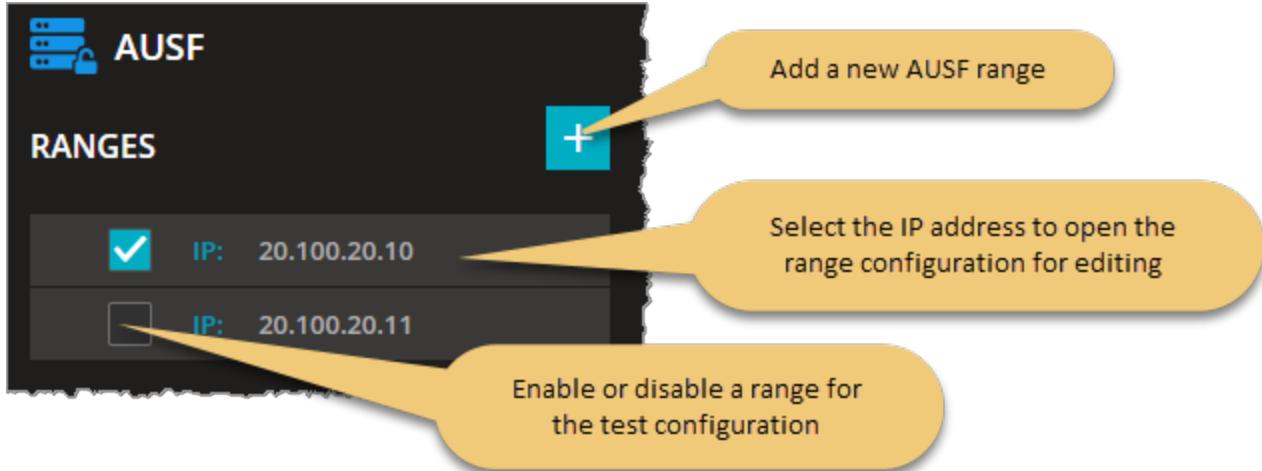
AUSF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



AUSF Range panel

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

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

AUSF range controls and settings

Each AUSF range is identified by a unique IP address. You can add and delete AUSF ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each AUSF 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 AUSF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the AUSF functionality (if

Setting	Description
	it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each AUSF range includes the configuration of an associated set of Node Settings, which are described in AUSF node settings below .
Nausf Interface Settings	Each AUSF range requires the configuration of Nausf interface settings, through which a AUSF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in AUSF Nausf interface settings on the next page .
Remote SBA Nodes	These settings are described in AUSF Remote SBA Nodes on page 103 .

AUSF node settings

Each AUSF range includes a set of Node Settings plus one or more associated Routing Indicators.

Node Settings

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

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

Routing Indicators

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.

You can add as many Routing Indicators as necessary to support your test objectives.

Setting	Description
	Select the Add Routing Indicator button to add a routing indicator for the AUSF range.
	Select the Delete button to remove the routing indicator from the AUSF range.

AUSF Nausf interface settings

Nausf is the service-based interface through which a AUSF instance makes its services available to other services in a 5G network.

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

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.

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

AUSF Remote SBA Nodes

UDM Connection Settings

To connect to the UDM node, the following configuration settings are required.

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the UDM node. This is the destination address of the UDM node to which the packets are sent over the Nudm interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nudm communications. It can be either HTTP or HTTPS.
Port	The UDM port number to use for Nudm communications. The default is port 80, but you can choose a different port number.
Use SCP Node	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the check box to enable it. For more details, refer to Use SCP.</p>

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.

Setting	Description
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

For several SBA nodes, if SCP is selected in SCP Connection Settings, a new option will be available:

- **Use SCP Node**

If SCP is selected in SCP Connection Settings, the messages will be forwarded to SCP on all the interfaces where SCP is supported. If **Use SCP Node** check box option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which the **Use SCP Node** check box is enabled will be forwarded to the SCP.

AMF configuration settings



Access and Mobility Management Function (AMF) is one of the fundamental components of the 5G core architecture. It provides UE-based authentication, authorization, and mobility management services. Some of the key AMF services include registration, connection, reachability, and mobility management. It also serves as termination points for RAN control-plane interface. It also supports transport of session management messages between UE and SMF.

AMF interacts with the RAN over the N2 reference point and makes its services available to other network functions through the Namf service-based interface.

The configuration settings are described in the topics listed below.

Topics:

AMF Ranges panel	106
AMF Range settings	107
AMF node settings	108
AMF N2 interface settings	111
AMF Namf interface settings	112
AMF N26 Interface Settings	112
AMF remote SBA nodes	113

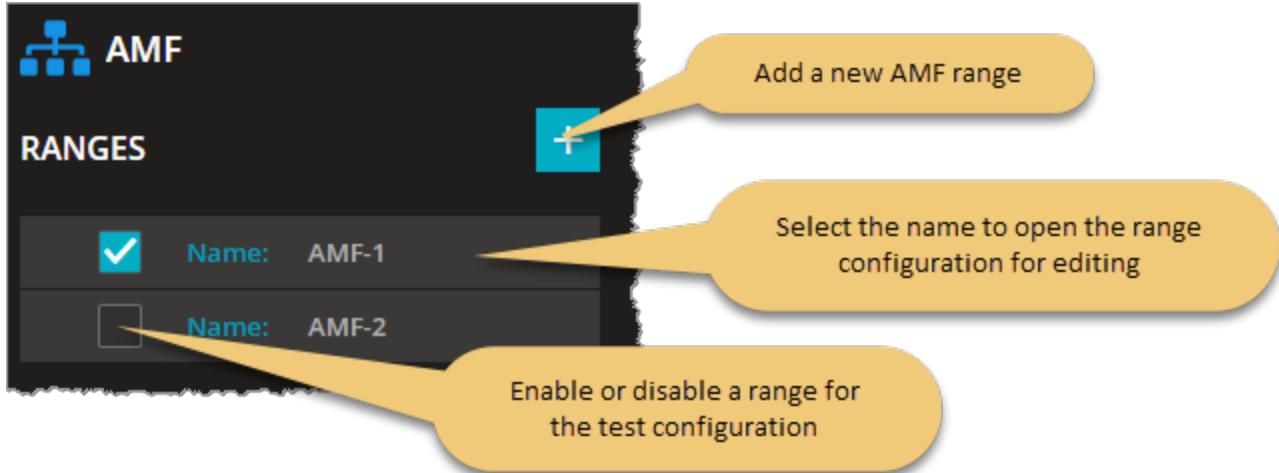
AMF Ranges panel

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

You can perform the following tasks from this 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 ...



AMF Range settings

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

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

AMF range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Device Under Test	Enable this option if your AMF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the AMF functionality (if it is selected in the Topology window).
<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 on the next page .
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, N14 and Namf interface settings.
Namf Interface Settings	Each AMF range requires the configuration of Namf interface settings, through which a AMF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in AMF N2, N14 and Namf interface settings.
N26 Interface Settings	In a 5G network, N26 is the interface between the MME and the AMF. These settings are described in AMF N26 Interface Settings on page 112 .
Remote SBA Nodes	These settings are described in AMF remote SBA nodes on page 113 .

AMF node settings

Each AMF range includes a set of Node Settings.

Node Settings

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

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

Setting	Description
	identifies the AMF Set within the AMF Region.
Pointer	The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.
Ciphering Algorithm	Allows to select the supported 5G ciphering algorithm: <ul style="list-style-type: none"> • NEA0 - Null ciphering algorithm • NEA1 - 128-bit SNOW 3G based algorithm • NEA2 - 128-bit AES based algorithm
Integrity Algorithm	Allows to select the supported 5G integrity protection algorithm: <ul style="list-style-type: none"> • NIA0 - Null Integrity Protection algorithm • NIA1 - 128-bit SNOW 3G based algorithm • NIA2 - 128-bit AES based algorithm
HTTP Connections	The number of HTTP connections between two nodes.
Request N2 SM Information	Select this check-box to request N2 SM Information again instead of using the existing one.
Establish UE Policy Association	Select this check-box to trigger Establishment of UE Policy Association to PCF. <div style="margin-left: 20px;"> NOTE UE Policy Association is not supported in tests configured with Idle or Handover objectives. </div> <div style="margin-left: 20px;"> NOTE Establish UE Policy Association is supported only when Technical Spec Version is R16 or higher. </div>
Prefer AMF Change	Select this check-box to change the AMF for an N2 handover even when the target RAN(T-RAN) is connected to the serving AMF.
<i>T3512: Select the check box to open T3512 Settings and configure the T3512 timer.</i>	
NOTE	<i>If disabled, a value of 50 minutes (Value 5 X Unit 10 minutes) is sent for T3512.</i>
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>

NSSAI

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

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

TAI

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

Setting	Description
<i>TAI:</i>	
	Select the Add TAI button to add a new TAI (Tracking Area Identity) to your test configuration.
<i>TAI settings:</i>	
	Select the Delete TAI button to delete this TAI from your test configuration.
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>	

Setting	Description
	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.

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.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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).
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.
Inner VLAN	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.

AMF Namf interface settings

Namf is the service-based interface through which a AMF instance makes its services available to other services in a 5G network.

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

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix 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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT 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.

AMF N26 Interface Settings

In a 5G network, N26 is the interface between the MME and the AMF. It supports interworking requirements between the EPC and the NG core.

You can enable or disable the N26 interface, as required by your test configuration. For example:



N26 Interface Settings

Setting	Description
Peer MME	Select the peer MME with which this AMF range will communicate over the N26 interface. All of the MME node ranges that you have enabled in the test are available for selection.
GTP-C UDP port	The UDP port to use for GTP-C messages. The default port is 2123, but you can use a different port.

Connectivity Settings

The following **Connectivity Settings** enable the necessary N26 connectivity between the AMF and the MME.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

AMF remote SBA nodes

- [AMF Connection Settings](#)
- [AUSF Connection Settings on page 115](#)

- [UDM Connection Settings on the facing page](#)
- [PCF Connection Settings on page 116](#)
- [SMF Connection Settings on page 116](#)
- [NRF Connection Settings on page 117](#)

AMF Connection Settings

N14 is the service-based interface through which an AMF instance interacts with another AMF instance in a 5G network, as described in TS 29518.

The N14 interface exposes the following messages associated to the N2 Handover with AMF change procedure:

- `Namf_Communication_CreateUEContext Request / Namf_Communication_CreateUEContext Response`
- `Namf_Communication_N2InfoNotify / Namf_Communication_N2InfoNotify Ack`

Currently, the N14 communication is supported only between two AMFs. Each of the configured AMF ranges has an implicit and unexposed count of 1 (this behavior is inherited).

One of the configured AMFs is emulated and the second AMF is configured as DUT (their order in the configuration is irrelevant).

AMFs have the possibility to configure a Peer AMF by selecting an option for the Peer AMF Type field:

- **None** - no N14 interface between AMFs (this is the default option)
- **Preset** - this option allows manually configuration of a peer AMF.

IMPORTANT If this option is selected, you can add **ONLY** one peer AMF.

This option requires the configuration of the peer AMF, as follows:

Setting	Description
<i>AMF Peers:</i>	
	Select this button to add the peer AMF to your test configuration.
<i>AMF Peer:</i>	
	Select this button to delete the peer AMF from your test configuration.
Peer AMF	Select the peer AMF from the drop-down list.
Protocol	The protocol to use for Namf communications. It can be either HTTP or HTTPS.
Port	The AMF port number to use for Namf communications. The default is port 80, but you can choose a different port number.

- **Discover** - this option relies on the NRF to assign the correct Peer AMF during the handover procedure. For this, AMFs must first register to the NRF using their [NSSAIs](#) and [TAIs](#).

NOTE

For legacy configurations, the NSSAI and TAI will be empty lists. In N14 tests, NSSAI and TAI configuration is mandatory. In order to have successful UE registrations, make sure the NSSAIs configured on the UE and AMF match.

IMPORTANT

The DUT AMF must have the correct GUAMI value configured (it should match the one configured on the actual AMF DUT). Otherwise, the N14 connection will not be established.

AUSF Connection Settings

To connect to the AUSF node, the following configuration settings are required.

Setting	Description
<i>AUSF Connectivity Settings:</i>	
Peer AUSF	<p>Select the peer AUSF using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the AUSF node. This is the destination address of the AUSF node to which the packets are sent over the Nausf interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nausf communications. It can be either HTTP or HTTPS.
Port	The AUSF port number to use for Nausf communications. The default is port 80, but you can choose a different port number.
Use SCP Node	<div style="background-color: #0070C0; color: white; padding: 2px 10px; display: inline-block;"> IMPORTANT </div> <p>This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the check box to enable it. For more details, refer to Use SCP.</p>

UDM Connection Settings

To connect to the UDM node, the following configuration settings are required.

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the UDM node. This is the destination address of the UDM node to which the packets are sent over the Nudm interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nudm communications. It can be either HTTP or HTTPS.

Setting	Description
Port	The UDM port number to use for Nudm communications. The default is port 80, but you can choose a different port number.
Use SCP Node	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the check box to enable it. For more details, refer to Use SCP.</p>

PCF Connection Settings

To connect to the PCF node, the following configuration settings are required.

Setting	Description
<i>PCF Connectivity Settings:</i>	
Peer PCF	<p>Select the peer PCF using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the PCF node. This is the destination address of the PCF node to which the packets are sent over the NPCf interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Npcf communications. It can be either HTTP or HTTPS.
Port	The PCF port number to use for Npcf communications. The default is port 80, but you can choose a different port number.

SMF Connection Settings

To connect to the SMF node, the following configuration settings are required.

Setting	Description
<i>SMF Connectivity Settings:</i>	
Peer SMF	<p>Select the peer SMF using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the SMF node. This is the destination address of the SMF node to which the packets are sent over the Nsmf interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nsmf communications. It can be either HTTP or HTTPS.
Port	The SMF port number to use for Nsmf communications. The default is port 80, but you can choose a different port number.

Setting	Description
Use SCP Node	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the check box to enable it. For more details, refer to Use SCP.</p>

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

For several SBA nodes, if SCP is selected in SCP Connection Settings, a new option will be available:

- **Use SCP Node**

If SCP is selected in SCP Connection Settings, the messages will be forwarded to SCP on all the interfaces where SCP is supported. If **Use SCP Node** check box option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which the **Use SCP Node** check box is enabled will be forwarded to the SCP.

DN configuration settings



Data Networks (DN) represents one of the entities in the 5G core network architecture. DN interfaces with UPF over the N6 reference point, enabling access to the public Internet, operator services, and other external data networks.

The configuration settings are described in the topics listed below.

Topics:

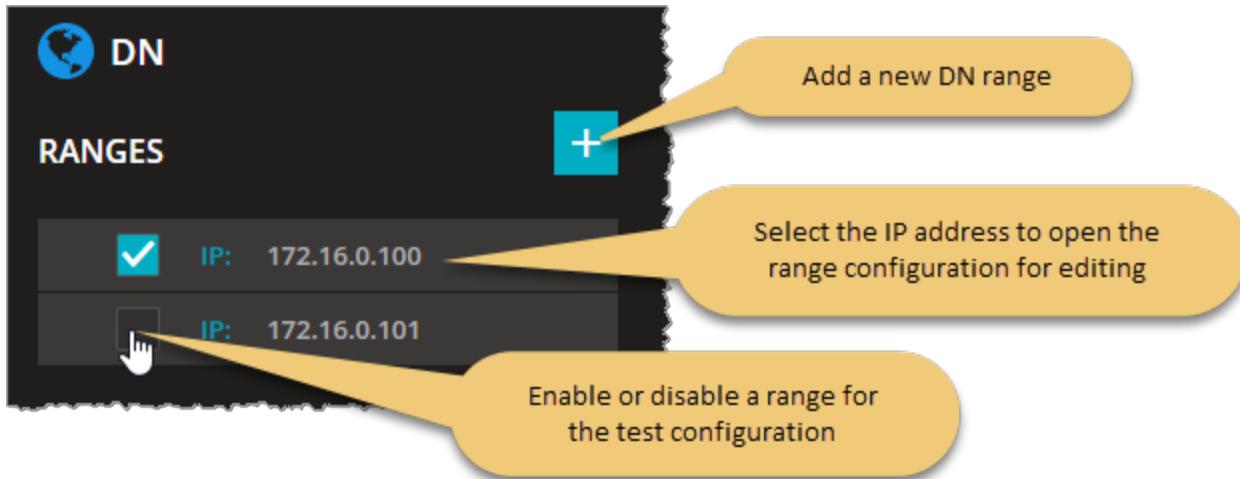
DN Ranges panel	119
DN Range panel	119
DN N6 interface settings	120
DN UE routes settings	121
DN User Plane	121
DN Application Traffic Generator	122
DN Stateless UDP Traffic Generator	129

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, LoadCore 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 **UE Routes Settings** to configure the route to an UE 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 below .
UE Routes Settings	These settings are described in DN UE routes settings on the facing page .
User Plane	These settings are described in DN User Plane on the facing page .

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.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

Connectivity 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	<p>IMPORTANT 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.

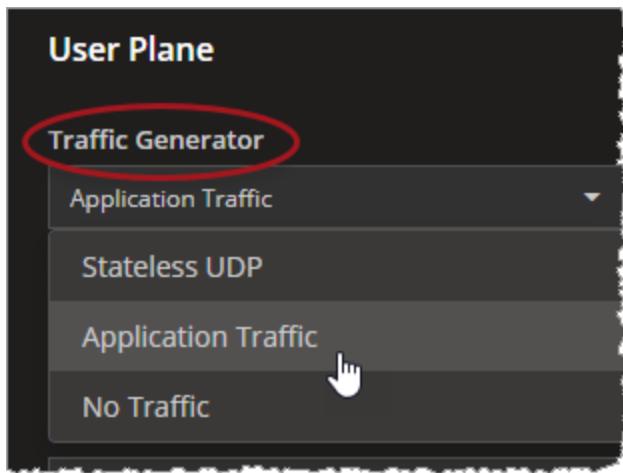
DN UE routes settings

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

Settings	Description
<i>UE Routes Config:</i>	
	Select this button to add a new route to a specific UE range.
<i>UE Routes Config:</i>	
	Select this button to remove the route to the UE range.
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.

DN User Plane

LoadCore provides two traffic generators: **Application Traffic** and **Stateless UDP** (plus a **No Traffic** option for tests that do no require user plane traffic):



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](#).

The DN settings required for the traffic generators are described in the following topics:

- [DN Application Traffic Generator below](#)
- [DN Stateless UDP Traffic Generator on page 129](#)

DN Application Traffic Generator

Use the **Application Traffic** generator to generate IP packets containing Layer 7 traffic for your test.



You can choose to generate Data Traffic, Voice Traffic or Ott Traffic, based on your test requirements.

The following table describes the Application Traffic generation parameters.

Parameter	Description
Address	The destination IP address for the user plane traffic that this UE range will generate.
	Select this button to add a new application traffic objective. The objective can be Data , Voice or Ott .
	Select this button to remove the application traffic objective from your test configuration.
Data	For the settings required to configure the Data traffic objective, refer to DN Data Traffic .
Voice	For the settings required to configure the Voice traffic objective, refer to DN Voice .

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

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 .
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>
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. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings. <p>Refer to Flow on the next page (below) for a description of the configuration settings for these traffic flows.</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	Select the L4/L7 protocol type from the list of pre-defined flows. The available Types include: <ul style="list-style-type: none"> HTTP Get and HTTP Put HTTPS Get and HTTPS Put FTP UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)
Port	The port used by the 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.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional.

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 .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated 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	The time (in milliseconds) to wait before the application traffic flows start.

Parameter	Description
traffic start (ms)	
Call Type	Select the type of call from the drop-down list. Available options are: <ul style="list-style-type: none"> • Basic Call • Basic Call Mo (Mobile Originated) • Basic Call Mt (Mobile Terminated)
Dial Plan:	<i>For the settings required to configure the dial plan, refer to Dial Plan.</i>
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore 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
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Media settings:	<i>For the configuration of media settings, refer to Media Settings.</i>

Dial Plan

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

Parameter	Description
Iterations	The number of times the Voice flow will be executed. It can be finite or infinite (set to zero).
Source Phone	The URI assigned to the first simulated user, incremented by 1 for each UE.
Destination Phone	The URI assigned to the first simulated user, incremented by 1 for each UE.
Destination IP	The destination IP address.
Destination Port	The destination port number.

Media Settings

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

Parameter	Description
Audio Duration (ms)	Length of time to play the audio stream. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID	The QoS Flow ID for RTP traffic. Select the QoS Flows ID(s) from the drop-down list.
<i>Jitter Buffer Settings:</i>	
Initial Delay (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-WD

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	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. <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	Indicates the mode(bitrate) of the AMR codec. For AMR there are 8 available modes. All these modes can be changed dynamically without negotiation, reflecting the main characteristics of this codec – adaptive rate. For AMR WB there are 9 modes available.

EVS

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

PCMU/PCMA/iLBC/G722/G723/G729

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

DN Ott Traffic

The following table describes the 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 Ott .
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).
<i>OTT Servers:</i>	
	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 LoadCore or overwrite it with your own value.
Transport	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • HTTP • HTTPS
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Streams:</i>	
	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

Parameter	Description
	the value provided by LoadCore or overwrite it with your own value.
URL	Set the URL path.
Type	Select the stream type from the drop-down list: <ul style="list-style-type: none"> • Real • Synthetic
Protocol	Select the protocol from the drop-down list: <ul style="list-style-type: none"> • Apple HLS • DASH. If the stream type is set to Synthetic , you can choose one protocol from list. If the stream type is set to Real , you will see the protocol of real stream loaded.
Stream Duration	If the stream type is set to Synthetic , you can configure the stream duration in seconds. If the stream type is set to Real , you will see the real stream duration.
Segment Duration	If the stream type is set to Synthetic , you can configure the segment duration in seconds. If the stream type is set to Real , you will see the real segment duration.
Quality Levels:	<i>Set the quality value for each level. The available options are: 500, 1000, 3000 and 5000 Kbps.</i> <i>If the stream type is set to Synthetic, you can configure maximum 8 quality levels specifying their bitrate in Kbps.</i> <i>If the stream type is set to Real, you will see the quality levels from the real stream.</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.

DN Stateless UDP Traffic Generator

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

Parameter	Description
<i>Stateless UDP Flows:</i>	
	Select the Add Flow button to add a downlink flow to the Stateless UDP Flows list.

Parameter	Description
<i>Flow:</i>	
	Select the Delete Flow button to remove this flow from the Stateless UDP Flows list.
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).
Payload Size	The size of the packet payload, in bytes.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .
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 on page 93 .
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>

MME configuration settings



In 4G EPC networks, the MME (Mobility Management Entity) manages UE session states, paging, mobility, roaming, and other bearer management functions. It is also the control node for the LTE access network, performing essential services such as bearer activation/deactivation, SGW selection for UEs, user authentication, idle mode tracking and paging, among other functions.

In the Full Core test topology, it communicates with the AMF over the N26 interface, with the RAN over the S1 interface, and with the SGW over the S11 interface.

The configuration settings are described in the topics listed below.

Topics:

MME Ranges panel	132
MME Range panel	132
MME node settings	134
MME S11 Interface Settings	135
MME N26 Interface Settings	136
MME S1 Interface Settings	137
MME S6a Interface Settings	139
MME Diameter	140

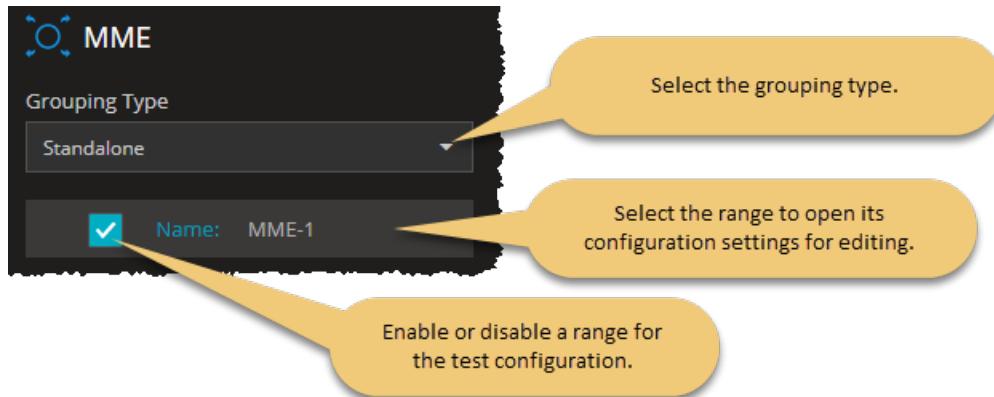
MME Ranges panel

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

You can perform the following tasks from this panel:

- Select the grouping type.
- Open the MME range configuration (for editing or viewing).
- Enable or disable the MME range for the test configuration.

For example...



The following configuration option is available on this panel:

Option	Description
Grouping Type	<p>This option determines the exposed simulated interfaces:</p> <ul style="list-style-type: none"> • Standalone: When selected, the topology exposes traffic sent over the S1-MME interface, capturing S1AP/NAS messages. <p>IMPORTANT If Grouping Type is set to Standalone for the MME, an agent must be assigned.</p> <ul style="list-style-type: none"> • With RAN
	<p>IMPORTANT To run a test using Standalone MME Grouping Type, the SGW Grouping Type must be set to With SMF or Standalone. For more details about SGW grouping, refer to SGW Ranges panel.</p>
	<p>IMPORTANT All the interfaces are enabled automatically if the MME Grouping Type is set to Standalone and the S1 interface IP configuration becomes mandatory.</p>

MME Range panel

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

- Delete the selected MME range from the test configuration.
- Designate the range as a **Device Under Test**.

- Select among the **Range Settings** to configure the node and interface settings for the MME range.

MME range controls and settings

Each MME range is identified by a unique range name. You can add and delete MME ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each MME 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 MME is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the MME functionality (if it is selected in the Topology window).
Range Count	The number of MMEs in the range.
<i>Range Settings:</i>	
Node Settings	Each MME range the configuration of an associated set of Node Settings, which are described in MME node settings on the next page .
S11 Interface Settings	Each MME range requires the configuration of S11 interface settings, through which an MME instance enables connectivity and interaction with SGW instances in the network. These settings are described in MME S11 Interface Settings on page 135 .
N26 Interface Settings	If your test requires 5G/4G interworking, then each MME range requires the configuration of N26 interface settings, through which an MME instance enables connectivity and interaction with AMF instances in the network. These settings are described in MME N26 Interface Settings on page 136 .
S1 Interface Settings	These settings are described in MME S1 Interface Settings on page 137 .
S6a Interface Settings	These settings are described in MME S6a Interface Settings on page 139 .
Diameter	These settings are described in MME Diameter on page 140 .

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
Name	A name uniquely identifies each MME range. You can accept the value provided by LoadCore or overwrite it with your own value.
Group ID	The MME Group Identifier to which this MME is assigned. The MME Group Identifier is a 16-bit value that is unique within a PLMN. The valid range of Group numbers is from 1 through 65535.
Code	The MME Code assigned to this MME. The MME Code is an 8-bit value that uniquely identifies an MME within an MME Group. The valid range of MME Code numbers is from 1 through 255.
PLMN MCC	The PLMN MCC for this MME 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 MME 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 Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.
Ciphering Algorithm	The supported 4G 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

Setting	Description
Integrity Algorithm	The supported 4G integrity 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

MME S11 Interface Settings

S11 is the control plane interface between an MME and an SGW.

You can enable or disable the S11 interface, as required by your test configuration. For example:



Interface Settings

The following settings are required to enable message transmission between this MME range and a selected SGW range.

Interface setting	Description
Peer SGW	Select an SGW range from the drop-down list. All of the SGW ranges that you have enabled for the test are available for selection.
GTP-C UDP port	Specify the UDP port number that will be used for GTP-C message transmission and receipt. The default port number is 2123, but you can select a different port as required by your test network.

Connectivity Settings

The following **Connectivity Settings** enable S11 connectivity between MME and SGW ranges.

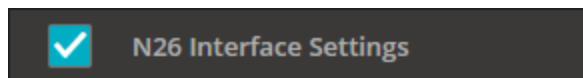
Connectivity setting	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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 setting	Description
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	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

MME N26 Interface Settings

In a 5G network, N26 is the interface between the MME and the AMF. It supports interworking requirements between the EPC and the NG core.

You can enable or disable the N26 interface, as required by your test configuration. For example:



Interface Settings

The following settings are required to enable message transmission between this MME range and a selected AMF range.

Interface setting	Description
Peer AMF	Select an AMF range from the drop-down list. All of the AMF ranges that you have enabled for the test are available for selection.
GTP-C UDP port	Specify the UDP port number that will be used for GTP-C message transmission and receipt. The default port number is 2123, but you can select a different port as required by your test network.

Connectivity Settings

The following **Connectivity Settings** enable N26 connectivity between MME and AMF ranges.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

MME S1 Interface Settings

The MME S1 interface IP configuration becomes mandatory when the MME Grouping Type is set to **Standalone**.

The following settings are required for the MME S1 interface:

S1 Interface setting	Description
Local SCTP port	The local 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.

Connectivity Settings

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

Connectivity setting	Description
	<i>VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.

MME S6a Interface Settings

S6a is a control-signaling interface that lies between the MME and the HSS. It enables transfer of subscription and authentication data for authenticating/authorizing user access to the evolved system (AAA interface) between the MME and HSS (as described in 3GPP TS 23.401).

You can enable or disable the S6a interface, as required by your test configuration. For example:



Interface Settings

The following settings are required to enable message transmission between this MME range and a selected HSS range.

Interface setting	Description
Peer UDM/HSS	Select the UDM/HSS range from the drop-down list. All of the UDM/HSS ranges that you have enabled for the test are available for selection.
Local SCTP port	The local 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.
Remote SCTP port	The remote SCTP port.

Connectivity Settings

The following **Connectivity Settings** enable S6a connectivity between MME and HSS ranges.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity setting	Description
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost

Connectivity setting	Description
	bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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	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.

MME Diameter

You can enable or disable Diameter, as required by your test configuration. For example:



The following settings are required to configure Diameter after enabling it.

Setting	Description
Origin Host Prefix	Set the origin host prefix. Default value: host .
Origin Realm	Set the origin realm. Default value: keysight.com .
Destination Host	Set the destination host prefix.
Destination Realm	Set the destination realm.

NRF configuration settings



Network Repository Function (NRF) is the 5G core network service that allows every network function to discover the services offered by other network functions. It supports the service discovery function by maintaining the set of NF profiles and the set of available NF instances. It makes its services available to other network functions through the Nnrf service-based interface. Multiple instances of NRF may be deployed, with each instance storing specific data.

Topics:

NRF Ranges panel	142
NRF Range panel	142
NRF node settings	143
NRF Nnrf interface settings	144

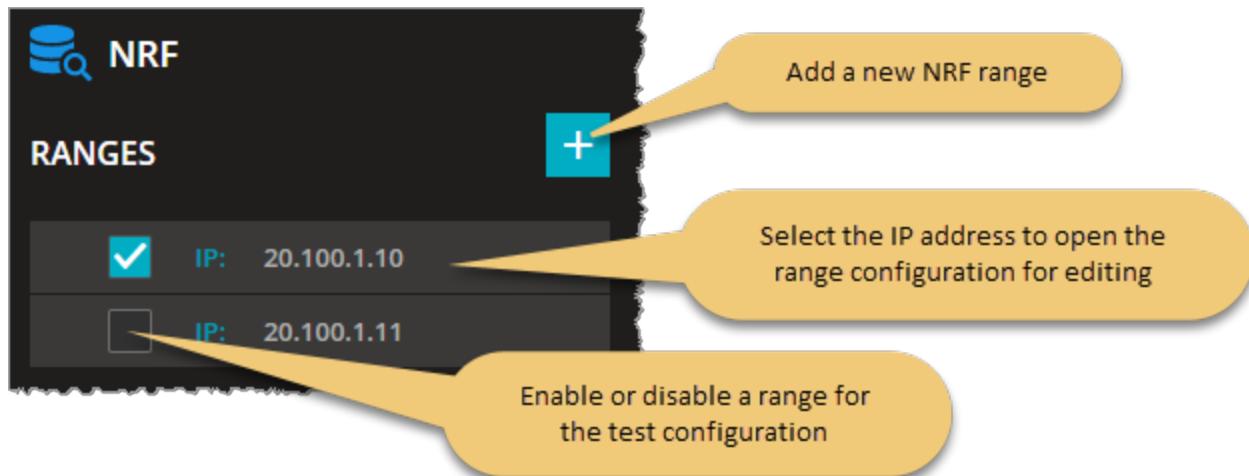
NRF Ranges panel

The **NRF Ranges** panel opens when you select the NRF node from the network topology window. Each NRF range is identified by a unique IP address that you configure.

You can perform the following tasks from this panel:

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

For example ...



NRF Range panel

When you select the IP address of a NRF range from the NRF Ranges panel, LoadCore opens the **Range** panel for that selected NRF. From that Range panel you can:

- Delete the selected NRF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the NRF range.

NRF range controls and settings

Each NRF range is identified by a unique IP address. You can add and delete NRF ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each NRF range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Device	Enable this option if your NRF is a DUT in this test configuration.

Setting	Description
Under Test	When this option is not enabled, the LoadCore will simulate the NRF functionality (if it is selected in the Topology window).

Range Settings:

Node Settings	Each NRF range includes the configuration of an associated set of Node Settings, which are described in NRF node settings below .
Nnrf Interface Settings	Each NRF range requires the configuration of Nnrf interface settings, through which a NRF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in NRF Nnrf interface settings on the next page .

NRF node settings

Each NRF range includes a set of Node Settings.

Node Settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple NRF instances may be deployed in the 5G network. Each NRF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
PLMN MCC	Set the mobile country code.
PLMN MNC	Set the mobile network code.
Heartbeat Interval(s)	Time in seconds expected between 2 consecutive heartbeat messages from an NF Instance to the NRF.

NRF Nnrf interface settings

Nnrf is the service-based interface through which a NRF instance makes its services available to other services in a 5G network.

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

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

SCP configuration settings



Service Communication Proxy (SCP) allows the user to use Indirect Communication between SBA nodes. As of now, only model C is supported which uses the `3gpp-Sbi-Target-apiRoot` custom header. Spec version R16 September 2020 is required to use this feature.

The Service Communication Proxy (SCP) enables an important role within the 5G Service Based Architecture (SBA), providing functions ranging from simplifying network topology by applying signaling aggregation and routing, to overload handling, message parameter harmonization and load balancing.

The configuration settings are described in the topics listed below.

Topics:

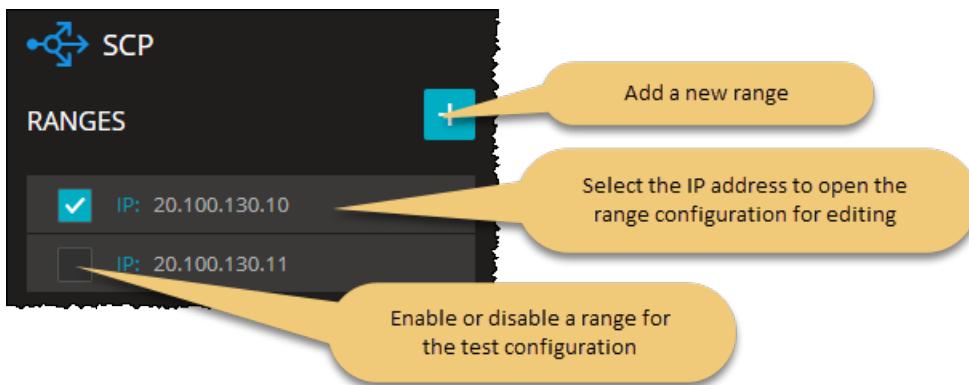
SCP Ranges panel	145
SCP Range panel	145
SCP interface settings	146
SCP Remote SBA Nodes	147

SCP Ranges panel

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

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

For example ...



SCP Range panel

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

- Select the **Delete Range** button to delete the selected SCP range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the SCP range.

SCP range controls and settings

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

The following table describes the available **Range** configuration options for each SCP 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 SCP is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the SCP functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	The SCP Node Settings are described below (Node Settings below).
SCP Interface Settings	Each SCP range requires the configuration of an interface necessary for SCP connectivity and use of indirect communication. These settings are described in SCP interface settings below .
Remote SBA Nodes	The remote SBA node settings are described in SCP Remote SBA Nodes on the facing page .

Node Settings

The following table describes the available SCP Node Settings.

Setting	Description
Instance ID	Each SCP instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
Forward to Another SCP	Select this check box to enable SCP Chaining. The SCP will be able to forward the messages it receives to a different SCP.
HTTP Connections	The number of HTTP connections between two nodes.

SCP interface settings

The following **Connectivity Settings** enable the necessary SCP connectivity and use of indirect communication.

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT 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.

SCP Remote SBA Nodes

Peer SCP Type

Setting	Description
None	When this option is selected, the SCP chaining is not used.
Preset	Select this option in order to use a specific IP for next SCP hop.
Discover	When this option is selected the SCP will send a request to NRF to discover the next hop SCP.

SCP Connection Settings

IMPORTANT These settings are available only when **Peer SCP Type** is set to **Preset**.

Setting	Description
Peer SCP	Select the IP address of the SCP node used as next hop.
Protocol	The protocol to use for communications. It can be either HTTP or HTTPS.
Port	The port number to use for communications. The default is port 80, but you can choose a different port number.

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

NSSF configuration settings



The Network Slice Selection Function (NSSF) selects Network Slice Instances (NSIs) based on information provided during UE attach. The NSSF offers services to the AMF (and to NSSFs to different PLMNs) via the Nnssf service based interface. N22 is the reference point between AMF and NSSF, and N31 is the reference point between the NSSF in the visited network and the NSSF in the home network.

The NSSF supports the following functionality:

- Selecting the set of Network Slice instances serving the UE
- Determining the Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs
- Determining the Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs
- Determining the AMF Set to be used to serve the UE

Topics:

NSSF Ranges panel	150
NSSF Range panel	150
NSSF node settings	151
Nnssf Interface Settings	152
Remote SBA nodes	153
NSSF Restricted NSSAIs	154
NSSF Network Slices	155
NSSF Configured NSSAI	156

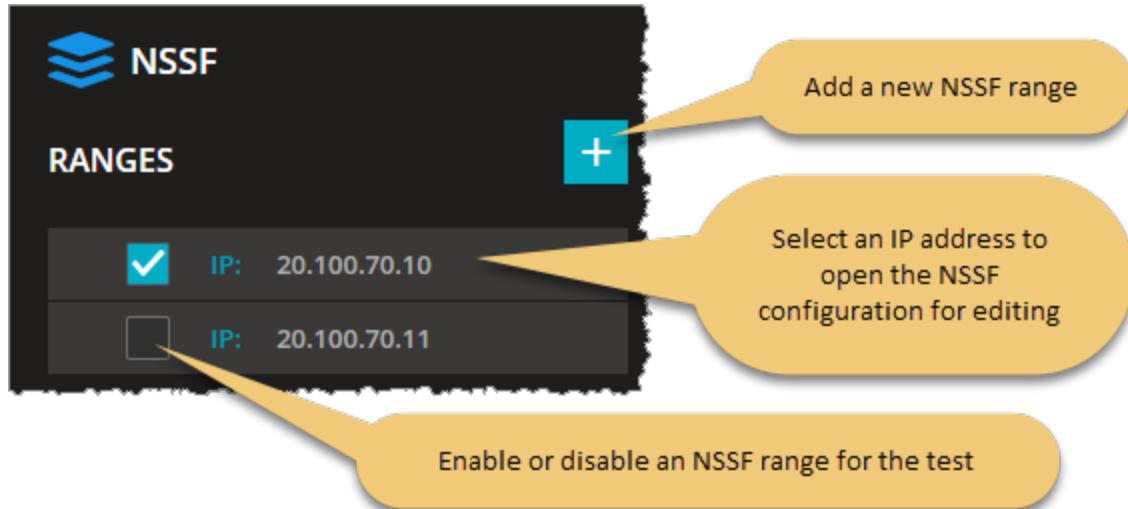
NSSF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



NSSF Range panel

Selecting an IP address from the NSSF **Ranges** panel provides access to the configuration settings on the **Range** panel. From the NSSF **Range** panel, you can:

- Delete the NSSF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node, Nnssf interface, and remote SBA nodes.
- Select **Network Slicing** to configure restricted NSSAIs, network slices, and configured NSSAIs.

NSSF range controls and settings

Each NSSF range is identified by a unique IP address. You can add and delete NSSF ranges as necessary to support your test requirements. The following table describes the **Range Settings** that you need to configure for each NSSF range.

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

Setting	Description
Device Under Test	Enable this option if your NSSF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the NSSF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each NSSF range requires the configuration of an associated set of Node Settings, which are described in NSSF node settings below .
Nnssf Interface Settings	Each NSSF range requires the configuration of Nnssf interface settings, through which a NSSF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in Nnssf Interface Settings on the next page .
Remote SBA Nodes	These settings are described in Remote SBA nodes on page 153 .
<i>Network Slicing:</i>	
Restricted NSSAIs	These settings are described in NSSF Restricted NSSAIs on page 154 .
Network Slices	These settings are described in NSSF Network Slices on page 155 .
Configured NSSAIs	These settings are described in NSSF Configured NSSAI on page 156 .

NSSF node settings

Each NSSF range includes a set of Node Settings. Each NSSF instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple NSSF instances may be deployed in the 5G network. Each NSSF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
PLMN MCC	Set the mobile country code. 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

Setting	Description
	<p>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>Set the mobile network code.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>

Nnssf Interface Settings

Nnssf is the service-based interface through which an NSSF instance makes its services available to other services in a 5G network.

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

Connectivity Setting	Description
<i>IP:</i>	
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The length of the IP prefix for this interface.
Gateway Address	The gateway address through which other servers will access this NSSF instance.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
<i>Outer VLAN:</i>	
Outer VLAN	Enable this option if you are using VLANs on this interface.
VLAN ID	The outer VLAN identifier.
<i>Inner VLAN:</i>	

Connectivity Setting	Description
Inner VLAN	<p>Enable this option if you are using VLANs on this interface and you need to configure inner VLANs.</p> <p>The Inner VLAN configuration settings are available only when <i>Outer VLAN</i> is enabled.</p>
VLAN ID	The inner VLAN identifier.

Remote SBA nodes

NRF Connection Settings

Selecting **Remote SBA Nodes** from the NSSF Range panel opens the **NRF Connection Settings** panel.

To connect to the NRF node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	<p>Select the IP address from your test network to use for Nnrf traffic. This is the destination address of the NRF node to which the packets are sent over the Nnrf interface.</p> <p>Select None if this NFFS range is not using the services of the NRF.</p>
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The NRF port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

NSSF Restricted NSSAIs

The AMF uses the NSSAI Availability Service to update the S-NSSAIs that the AMF supports on a per-TA basis on the NSSF and to subscribe and notify any status changes, on a per-TA basis, of the S-NSSAIs available per TA (unrestricted) and the restricted S-NSSAI(s) per PLMN in that TA in the serving PLMN of the UE.

You use the **NSSF Restricted NSSAIs** settings to define the Restricted NSSAIs for your test. For each Restricted NSSAI in your configuration, you will configure one or more Restricted S-NSSAIs.

Setting	Description
<i>Restricted NSSAIs:</i>	
	Select the Add a restricted NSSAI button to add a restricted NSSAI to your test configuration.
<i>Restricted NSSAI settings:</i>	
	Select the Delete Restricted NSSAI button to delete this NSSAI from your test configuration.
<i>Tracking Area Identity (TAI):</i>	
MCC	The PLMN MCC that is used in the construction of this TAI.
MNC	The PLMN MNC that is used in the construction of this TAI.
TAC	The PLMN TAC that is used in the construction of this TAI.
<i>Restricted S-NSSAIs:</i>	
	Select the Add NSSAI button to add a Restricted A-NSSAI to your test configuration.
<i>NSSAI Settings:</i>	
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default 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 default Mapped configured Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The default Mapped configured Slice Differentiator (SD) value for this S-NSSAI.

NSSF Network Slices

You use the **NSSF Network Slices** settings to configure one or more network slices for use in your test. A network slice is a 5G logical network that provides specific network capabilities and network characteristics.

Setting	Description
<i>Network Slices:</i>	
	Select the Add a Network slice button to add a network slice to your test configuration.
<i>Network Slice settings:</i>	
	Select the Delete a Network Slice button to remove this network slice from your test configuration.
Slice Name	Each network slice is uniquely identified by a <i>Slice Name</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Slice NRF (Network Repository Function):</i>	
Slice NRF host	The identifier (IP address) of the Network Repository Function (NRF) host to be used to select services within a Network Slice instance.
Protocol	The protocol used for communications. You can choose either HTTP or HTTPS.
Port	The port number used for communications. The default is port 80, but you can choose a different port number.
<i>Tracking Areas:</i>	
	Select the Add Tracking Area button to add a Tracking Area (TA) to your test configuration.
<i>Tracking Area Indication (TAI) settings:</i>	
	Select the Delete TAI button to delete this TAI from your test configuration.
MCC	The Mobile Country Code (MCC) used in the construction of the TAI.
MNC	The Mobile Network Code (MNC) used in the construction of the TAI.
TAC	The Tracking Area Code (TAC) used in the construction of the TAI.

NSSF Configured NSSAI

You use the **NSSF Configured NSSAI** settings to define one or more Configured NSSAIs for your test configuration. A Configured NSSAI is an NSSAI with which the PLMN may configure a UE, in which case the UE will use it as the default NSSAI.

Setting	Description
<i>Configured NSSAI:</i>	
	Select the Add a Configured NSSAI button to add a Configured NSSAI to your test configuration.
<i>Configured SNSSAI settings:</i>	
	Select the Delete a Configured NSSAI button to remove this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The default Mapped configured Slice/Service Type (SST) value for this NSSAI.
Mapped SD	The default Mapped configured Slice Differentiator (SD) value for this NSSAI.
Slice names	Select from among the available slice names (the slices that you defined using the NSSF Network Slices settings). There is also an option to select all of the slices.

PCF/PCRF configuration settings



PCF/PCRF

Policy Control Function (PCF) is the 5G core network component that governs the network behavior by supporting unified policy framework. It provides policy rules to Control Plane function(s). This includes network slicing, roaming, and mobility management. Also, it accesses subscription information for policy decisions taken by the UDR. It makes its services available to other network functions through the Npcf service-based interface. Multiple instances of PCF may be deployed, with each instance storing specific data.

Policy and Charging Rules Function (PCRF) is the software node designated in real-time to determine policy rules in a multimedia network. It operates at the network core and accesses subscriber databases and other specialized functions, such as a charging system, in a centralized manner.

The configuration settings are described in the topics listed below.

Topics:

PCF Ranges panel	158
PCF Range panel	159
PCF node settings	160
PCRF node settings	161
PCF service area restrictions	161
PCF Npcf interface settings	162
PCRF Rx interface settings	163
PCF remote SBA nodes	164

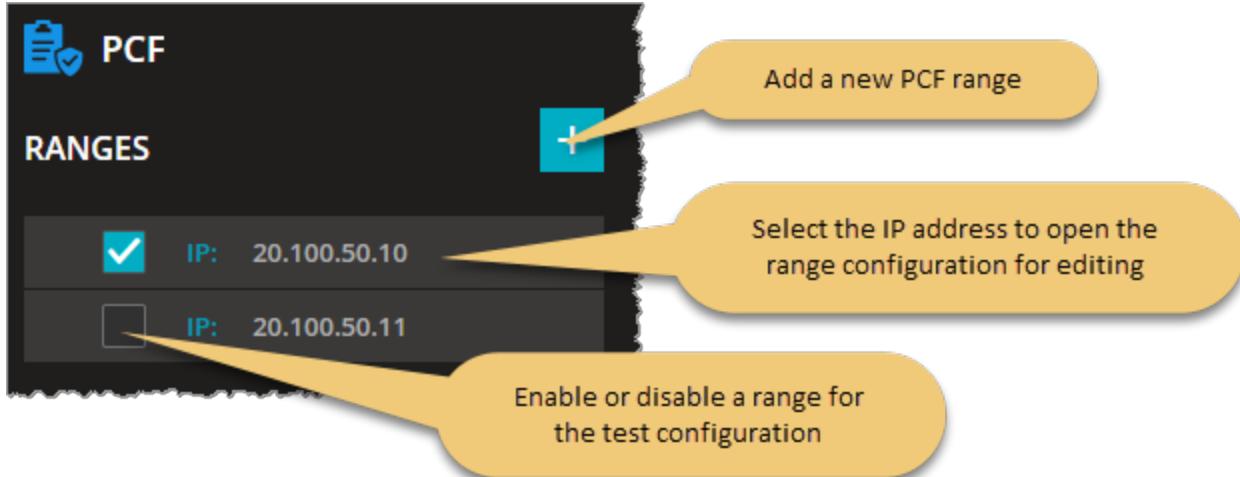
PCF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



PCF Range panel

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

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

PCF range controls and settings

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

The following table describes the **Range Settings** that you need to configure for each PCF 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 PCF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the PCF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each PCF range the configuration of an associated set of Node Settings, which are describe in PCF node settings on the next page .
PCRF Node Settings	
Service Area Restrictions	Each PCF range requires the configuration of the service area restrictions. The settings are described in PCF service area restrictions on page 161 .
Npcf Interface Settings	Each PCF range requires the configuration of Npcf interface settings, through which a PCF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in PCF Npcf interface settings on page 162 .
Rx Interface Settings	
Remote SBA Nodes	These settings are described in PCF remote SBA nodes on page 164 .

PCF node settings

Each PCF range includes a set of Node Settings.

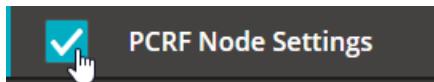
Node Settings

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

Setting	Description
Instance ID	<p>Multiple PCF instances may be deployed in the 5G network.</p> <p>Each PCF instance is uniquely identified by an <i>Instance ID</i>. You can accept the value provided by LoadCore or overwrite it with your own value.</p>
PLMN MCC	<p>The PLMN MCC for this PCF 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 PCF 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>
RFSP	The value of RAT/Frequency Selection Priority (RFSP) index.
Triggers	<p>Request Triggers to which the PCF subscribes. The allowed values are:</p> <ul style="list-style-type: none"> • Location Change (tracking area). The tracking area of the UE has changed. • PRA Change (change of UE presence in PRA). The UE is entering/leaving a Presence Reporting Area. <p>Both values can be selected simultaneously.</p>
Include Request in Response	Select the check-box to include the request in the response message.

PCRF node settings

You can enable or disable the PCRF node settings interface, as required by your test configuration. For example:



The following settings are required to configure the PCRF node.

Setting	Description
Origin Host Prefix	Set the origin host prefix. The default value is host .
Origin Realm	Set the origin realm. The default value is keysight.com .
Destination Host	Set the destination host.
Destination Realm	Set the destination realm.

PCF service area restrictions

The policy information sent from the PCF to AMF may contain service area restrictions for the UE. This means that the UE's access to the network resources can be restricted or limited.

The following configuration settings are required in order to define service area restrictions.

Setting	Description
<i>Service Area Restrictions:</i>	
Restriction type	Set the restriction type attribute: <ul style="list-style-type: none"> Allowed Areas Not Allowed Areas
Max No. Of TAs	The maximum number of allowed TAs that can be traversed.

Areas

The following configuration settings are required in order to define the tracking area identities.

For each PCF range in your test configuration, you can add and delete AREAS as required to meet your test objectives.

Setting	Description
<i>Areas:</i>	
	Select the Add Area button to add a new restriction area to your configuration.

Setting	Description
<i>Area:</i>	
	Select the Delete Area button to remove the restriction area from your configuration.
Area Codes	<p>Set the area code.</p> <p>Location Area Code (LAC) is a fixed length code (two octets) identifying a location area within a PLMN.</p>
<i>TACS:</i>	
	<p>This represents the Tracking Area Code (TAC) for this eNodeB. Select the Add TAC button to add a new TAC to your configuration.</p> <p>A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).</p>
	Select the Delete button to remove the tracking area code from your configuration.

After configuring it, the Service Area Restriction information consists of:

- either:
 - the maximum number of allowed TAs that can be traversed encoded as Max No. Of TAs attribute, and/or
 - both of :
 - a list of allowed Tracking Area Identities (TAIs) encoded as TACS attributes within the AREA attribute
 - the restriction type attribute set to Allowed Areas
- or:
 - a list of not allowed Tracking Area Identities (TAIs) encoded as TACS attributes within the AREA attribute, and
 - the restriction type attribute set to Not Allowed Areas

PCF Npcf interface settings

Npcf is the service-based interface through which a PCF instance makes its services available to other services in a 5G network. The following **Connectivity Settings** enable the necessary Npcf connectivity and service interaction.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT 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.

PCRF Rx interface settings

NOTE

the Rx interface settings are enable and can be configured only when the **PCRF node settings** check box is selected.

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

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

Connectivity Settings	Description
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Port	The port number to use for this interface communications.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

PCF remote SBA nodes

UDR Connection Settings

The Unified Data Repository (UDR) stores policy data that is used by the PCF.

To connect to the UDR node, the following configuration settings are required.

Setting	Description
<i>UDR Connectivity Settings:</i>	
Peer UDR	<p>Select the peer UDR using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the UDR node. This is the destination address of the UDR node to which the packets are sent over the Nudr interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nudr communications. It can be either HTTP or HTTPS.
Port	The UDR port number to use for Nudr communications. The default is port 80, but you can choose a different port number.

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

RAN 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 Full Core 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.

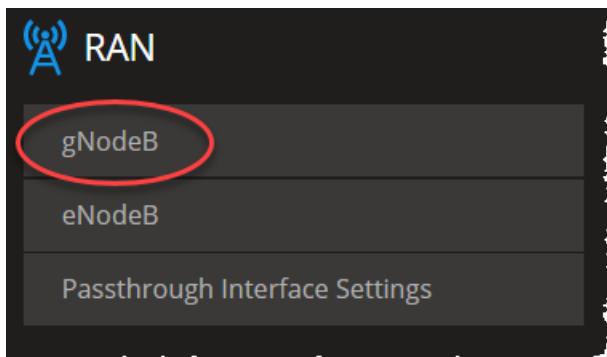
The configuration settings are described in the topics listed below.

Topics:

gNodeB	167
gNodeB Ranges panel	168
gNodeB Range settings	172
gNodeB node settings	173
gNodeB NSSAI settings	174
gNodeB N2 interface settings	175
gNodeB N3 interface settings	177
eNodeB	179
eNodeB Ranges panel	180
eNodeB Range Settings	180
eNodeB Node Settings	181
S1 Interface Settings	182
S1-U Interface Settings	183
Passthrough interface settings	185

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	168
gNodeB Range settings	172
gNodeB node settings	173
gNodeB NSSAI settings	174
gNodeB N2 interface settings	175
gNodeB N3 interface settings	177

gNodeB Ranges panel

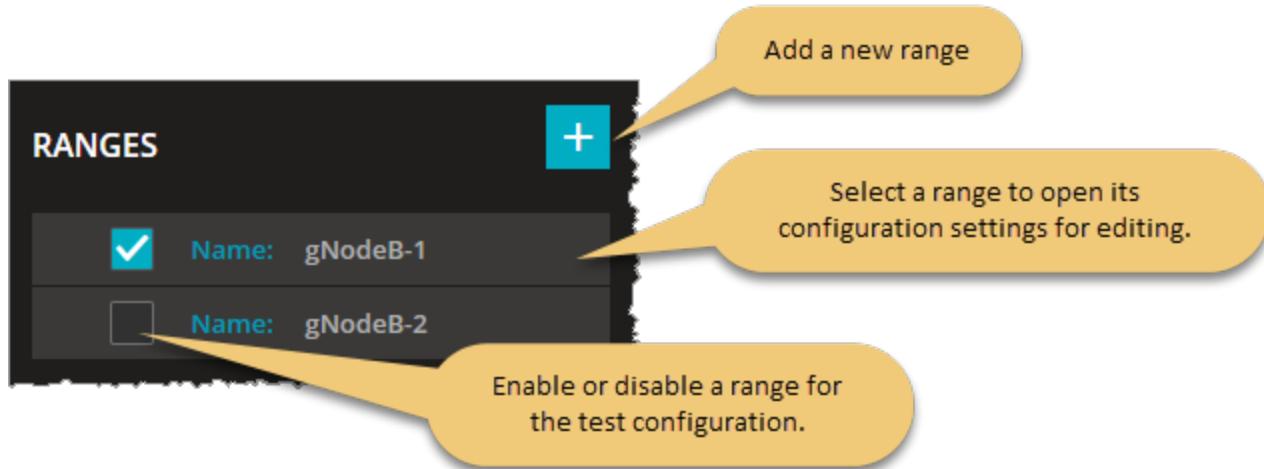
The **gNodeB Ranges** panel opens when you select **gNodeB** from the RAN pane. It consists of two main section: Ranges and Ranges Connectivity.

Ranges

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

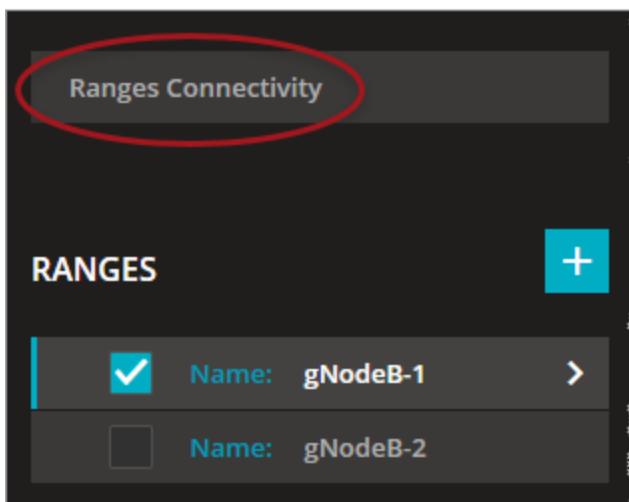
- Add a new gNodeB range to your test configuration.
- Open a gNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

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, LoadCore 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.

	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4
gNodeB-1				
gNodeB-2	<input type="checkbox"/>			
gNodeB-3	<input checked="" type="checkbox"/>	<input type="checkbox"/>		
gNodeB-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

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.

If there are some disabled gNodeB ranges then a specific message is displayed on hovering the cell on the line of that gNodeB range or the column of that gNodeB range.

For example ...

The gNodeB-4 range is a disabled range and when one cell of gNodeB-4 line (or gNodeB-4 column) is hovered a message is displayed in a tooltip to announce that gNodeB-4 is disabled.

	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6	gNodeB-7
gNodeB-1							
gNodeB-2	<input type="checkbox"/>						
gNodeB-3	<input type="checkbox"/>	<input type="checkbox"/>					
gNodeB-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
gNodeB-5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
gNodeB-6	<input type="checkbox"/>						
gNodeB-7	<input type="checkbox"/>						

NOTE

Once 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.

RANGES	+/-	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6	gNodeB-7
		gNodeB-1						
		gNodeB-2	<input type="checkbox"/>					
		gNodeB-3	<input type="checkbox"/>	<input type="checkbox"/>		gNodeB-4 is disabled		
		gNodeB-4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
		gNodeB-5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		gNodeB-6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		gNodeB-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 tooltip message on the hovered cell between gNodeB-3 and gNodeB-4 is updated displaying both gNodeB ranges as being disabled.

RANGES	+/-	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6	gNodeB-7
		gNodeB-1						
		gNodeB-2	<input type="checkbox"/>					
		gNodeB-3	<input type="checkbox"/>		gNodeB-3 and gNodeB-4 are disabled			
		gNodeB-4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>			
		gNodeB-5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		
		gNodeB-6	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
		gNodeB-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

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 or Minus(-) you can select it to change the state to Checked and all Xn links from the connectivity matrix will become selected (all connected).
Minus(-)	Indeterminate	

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

The screenshot shows the 'Ranges Connectivity' interface. On the left, there's a list of gNodeB ranges with checkboxes next to their names. Most ranges have their checkboxes checked, except for 'gNodeB-3' and 'gNodeB-4'. To the right is a 7x7 matrix representing the connectivity between these gNodeB ranges. Every cell in the matrix contains a checkbox, and all of them are checked, indicating that every Xn link between any two gNodeB ranges is selected.

	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6	gNodeB-7
gNodeB-1							
gNodeB-2	<input checked="" type="checkbox"/>						
gNodeB-3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>					
gNodeB-4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
gNodeB-5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
gNodeB-6	<input checked="" type="checkbox"/>						
gNodeB-7	<input checked="" type="checkbox"/>						

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, LoadCore 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 LoadCore 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 described in gNodeB node settings on the facing page .
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 on page 174 .
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 on page 175 .
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 N2 interface settings on page 175 .

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 LoadCore 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 code	The Tracking Area Code to use for the nodes in this range.
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, LoadCore increments the <i>gNodeB ID</i> setting for each gNodeB. (<i>Range Count</i> is one of the gNodeB Range settings on the previous page .)
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.

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
5QI	Select the 5G QoS identifier that will trigger the EPS fallback procedure. (The 5QI must be defined on the QoS Flow configuration settings on page 93 panel in the Global Settings .) When a request is received for this 5QI to create a dedicated QoS flow, the RAN will

Setting	Description
	reject the request, which will trigger the EPS fallback procedure.
Associated ENB	Select the eNodeB used for handover.
EPS Fallback Return Mobility	Select an option from the drop down list: <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.

gNodeB NSSAI settings

Each UE range requires at least one NSSAI range.

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

The slice assistance information comprises a list of one or more NSSAIs, 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 NSSAIs (NASSAI 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
<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	<p>The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:</p> <table border="1"> <thead> <tr> <th>SST</th> <th>Value</th> <th>Suitable for handling:</th> </tr> </thead> <tbody> <tr> <td>eMBB</td> <td>1</td> <td>5G enhanced Mobile Broadband</td> </tr> <tr> <td>URLCC</td> <td>2</td> <td>ultra-reliable low-latency communications</td> </tr> <tr> <td>MIoT</td> <td>3</td> <td>massive IoT</td> </tr> </tbody> </table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
SST	Value	Suitable for handling:											
eMBB	1	5G enhanced Mobile Broadband											
URLCC	2	ultra-reliable low-latency communications											
MIoT	3	massive IoT											
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the NSSAI.												
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 N2 interface is disabled, the gNodeB node can not be used as [Parent Node](#) for an UE range or as a hop in visited nodes list for the [Handover](#) objective.

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	The destination Stream Control Transmission Protocol (SCTP) port for control

Settings	Description
port	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.

Connectivity Settings

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).
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.
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>

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

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.

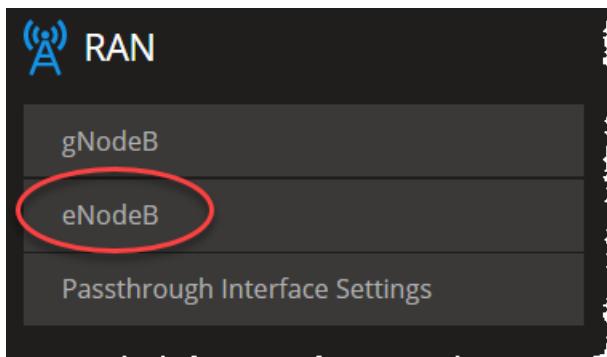
NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

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

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:

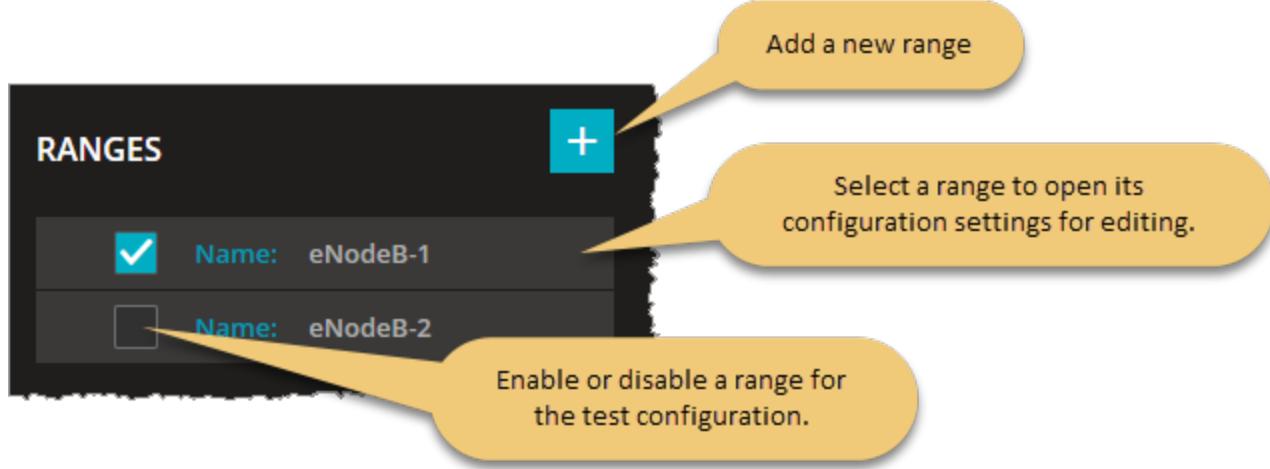
eNodeB Ranges panel	180
eNodeB Range Settings	180
eNodeB Node Settings	181
S1 Interface Settings	182
S1-U Interface Settings	183

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 ...



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 on the facing page .
S1 Interface Settings	Each eNodeB range requires the configuration of an associated set of S1 Interface Settings, which are described in S1 Interface Settings on page 182 .

Setting	Description
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 on page 183 .

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 LoadCore 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, LoadCore increments the <i>eNodeB ID</i> setting for each eNodeB. (<i>Range Count</i> is one of the eNodeB Range Settings on the previous page .)
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.

S1 Interface Settings

The **S1 Interface Settings** should be enabled and configured when the test is not simulating the MME. When LoadCore 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 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 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.

Connectivity Settings

The following table describes the parameters that you need to configure for the connectivity settings:

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

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

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 LoadCore 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

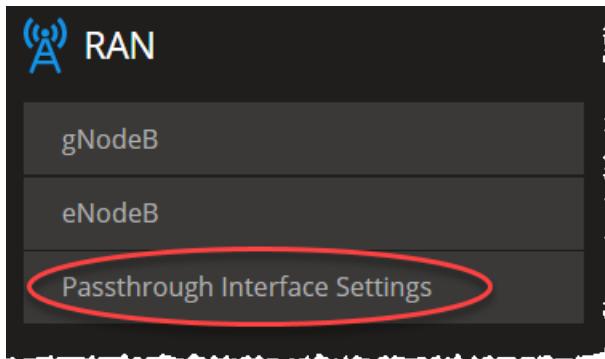
NOTE The following connectivity settings are available in LoadCore Web interface, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>

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

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
<i>IP</i>	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.
<i>MAC</i>	Select the MAC address to open the MAC configuration panel for editing.
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
<i>Outer VLAN</i>	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.

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

SGW configuration settings



In 4G EPC networks, the SGW (Serving Gateway) is the user plane node responsible for forwarding and routing packets between the eNodeB and the packet data network gateway (PGW). It also serves as the local mobility anchor for mobility between 3GPP networks and for inter-eNodeB handovers.

In the Full Core test topology, it communicates with the SMF/PGW-C node over the S5-c interface, with the UPF/PGW-U over the S5-u interface, with the RAN over the S1-u interface, and with the MME over the S11 interface.

The configuration settings are described in the topics listed below.

Topics:

SGW Ranges panel	188
SGW Range panel	188
SGW S1-U Interface Settings	190
SGW S5-C Interface Settings	191
SGW S5-U Interface Settings	192
SGW S11 Interface Settings	193
SGW DUT S11 Interface Settings	194

SGW Ranges panel

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

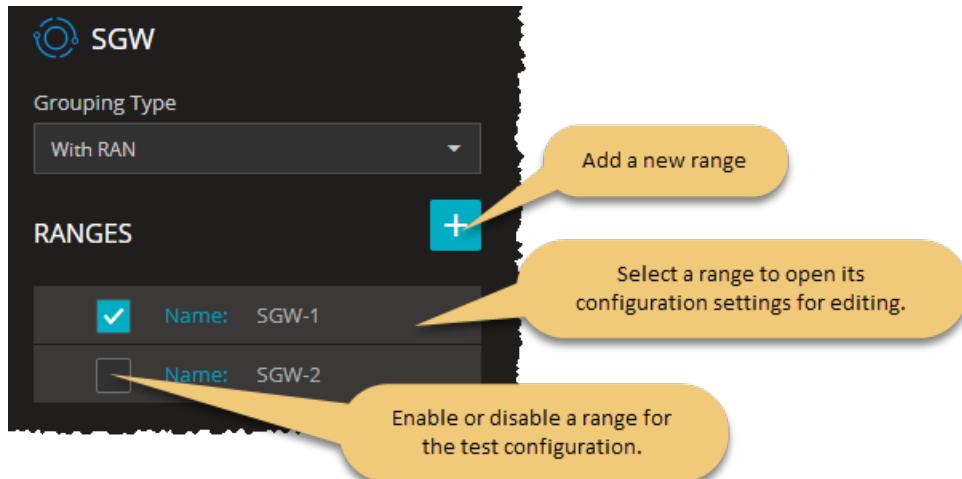
The following configuration option is available on this panel:

Option	Description
Grouping Type	<p>This option determines the exposed simulated interfaces:</p> <ul style="list-style-type: none"> • With RAN: When selected, the topology exposes the S5-c and S5-u interfaces. • With SMF: When selected, the topology exposes the S11 interface. • Standalone: When selected, the topology exposes: <ul style="list-style-type: none"> ▪ DUT S11 interface if the SGW range is placed under test (Device Under Test check-box is selected). ▪ S1-u, S5-c, S5-u and S11 interfaces if the SGW range is simulated (Device Under Test check-box is NOT selected).

In addition, you can perform the following tasks from this panel:

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

For example...



IMPORTANT

A Middleware validation prevents the user to run a configuration where any of the following secondary objectives: **Handover**, **Paging**, **Enter/Exit Idle**, **SMS**, are used in a test with SGW standalone (DUT or simulated).

SGW Range panel

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

- Delete the selected SGW range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select among the **Range Settings** to configure the node and interface settings for the SGW range.

SGW range controls and settings

Each SGW range is identified by a unique range name. You can add and delete SGW ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each MME 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 SGW is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the SGW functionality (if the SGW range is selected in the Topology window).
<i>Range Settings:</i>	
UDP Rx Buffer (bytes)	<p>IMPORTANT This field is available only when the Grouping Type is set to Standalone and the SGW range is simulated.</p> <p>Size of receive buffers for UDP sockets:</p> <ul style="list-style-type: none"> • minimum: 212992 #The default Linux buffer size • maximum: 134217728 #128MB • default: 12582912 #12MB
UDP Tx Buffer (bytes)	<p>IMPORTANT This field is available only when the Grouping Type is set to Standalone and the SGW range is simulated.</p> <p>Size of transmit buffers for UDP sockets:</p> <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 on the next page .
S5-c Interface Settings	Each SGW range requires the configuration of the S5-C interface, over which an SGW-C instance communicates with a PGW-C instance in the network. These settings are described in SGW S5-C Interface Settings on page 191 .
S5-u Interface	Each SGW range requires the configuration of the S5-U interface, over which an SGW-U instance communicates with a PGW-U instance in the network. These

Setting	Description
Settings	settings are described in SGW S5-U Interface Settings on page 192 .
S11 Interface Settings	These settings are described in SGW S11 Interface Settings on page 193 .
DUT S11 Interface Settings	These settings are described in SGW DUT S11 Interface Settings on page 194 .

SGW-C and SGW-U, introduced in 3GPP Release 14 as part of the Control and User Plane Separation strategy (CUPS), respectively handle the control plane and user plane forwarding responsibilities in 4G networks.

SGW S1-U Interface Settings

The S1 user plane external interface (S1-U) connects the eNodeB to the Serving Gateway (SGW) and is used to transmit user data on to the Packet Gateway and the internet.

Connectivity Settings

The following **Connectivity Settings** enable S1-U interface connectivity in your test network.

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

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

SGW S5-C Interface Settings

S5-C is the interface between the SGW-C node and PGW-C node in a 3GPP Release 14 network.

Connectivity Settings

The following **Connectivity Settings** enable S5-C interface connectivity in your test network.

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

Connectivity setting	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.

SGW S5-U Interface Settings

S5-U is the interface between the SGW-U node and PGW-U node in a 3GPP Release 14 network.

Connectivity Settings

The following **Connectivity Settings** enable S5-U interface connectivity in your test network.

Connectivity setting	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).
<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>	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.

SGW S11 Interface Settings

S11 is the control plane interface between an MME and an SGW.

Interface Settings

The following settings are required to enable message transmission between the selected SGW range and MME.

Interface setting	Description
GTP-C UDP port	Specify the UDP port number that will be used for GTP-C message transmission and receipt. The default port number is 2123, but you can select a different port as required by your test network.

Connectivity Settings

The following **Connectivity Settings** enable S11 connectivity between MME and SGW ranges.

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

Connectivity setting	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.

SGW DUT S11 Interface Settings

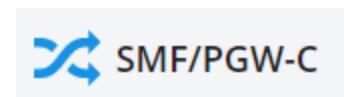
S11 is the control plane interface between an MME and an SGW.

Interface Settings

The following settings are required to enable message transmission between the selected SGW range and MME.

Interface setting	Description
S11 IP Address	The IP address from your test network to use for traffic on this interface.

SMF/PGW-C configuration settings



Session Management Function (SMF), as the name implies, handles management of UE sessions while also allocating IP addresses to UEs. It also selects and controls the UPF for data transfer. Per-session SMFs may be allocated to UEs with multiple sessions. It also interacts with the User Plane Function (UPF) for efficient routing of the user's packets.

SMF interacts with the UPF over the N4 reference point and makes its services available to other network functions through the Nsmf service-based interface.

The PGW-C controls the functionality performed by the assigned PGW-U when Control and User Plane Separation (CUPS) is in place. When a subscriber establishes an EPS (Evolved Packet System) bearer to a given PDN, the PGW-C selects and controls the point of attachment to that PDN for the life of the EPS bearer. Responsibilities include resource management for bearer resources, bearer binding, subscriber IP address management and mobility support.

The configuration settings are described in the topics listed below.

Topics:

SMF/PGW-C Ranges panel	196
SMF/PGW-C Range settings	197
SMF node settings	198
SMF N4 interface settings	199
SMF Nsmf interface settings	200
SMF remote SBA nodes	201

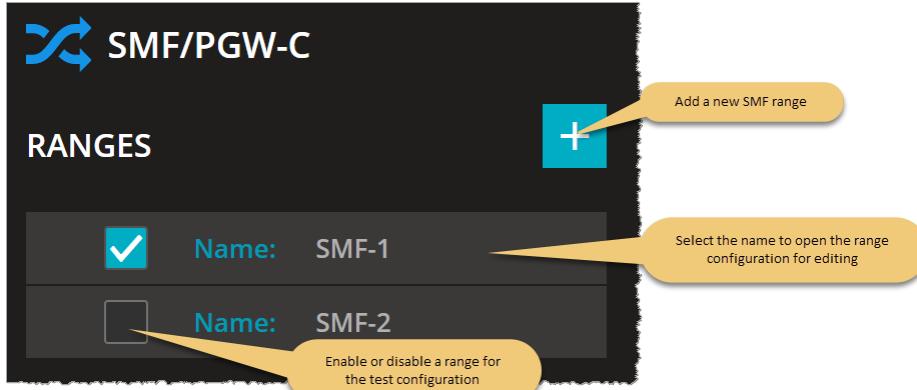
SMF/PGW-C Ranges panel

The **SMF/PGW-C Ranges** panel opens when you select the SMF node from the network topology window.

You can perform the following tasks from this panel:

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

For example ...



SMF/PGW-C Range settings

You add and select SMF ranges from the SMF/PGW-C Ranges panel. When you select the name of a SMF, LoadCore opens the **Range** panel, from which you can:

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

SMF range controls and settings

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

The following table describes the **Range Settings** that you configure for each SMF 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 SMF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the SMF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each SMF range requires the configuration of an associated set of Node Settings, which are described in SMF node settings on the next page .
N4 Interface Settings	Each SMF range requires the configuration of N4 interface settings, through which a SMF instance interacts with UPF in a 5G network. These settings are described in SMF N4 and Nsmf interface settings.
Nsmf Interface Settings	Each SMF range requires the configuration of Nsmf interface settings, through which a SMF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in SMF N4 and Nsmf interface settings.
S5-c Interface Settings	This interface is enabled only if the associated checkbox is selected. S5-c is the interface between the S-GW and P-GW. The interface settings are described in SMF S5-c interface settings .
Remote SBA Nodes	These settings are described in SMF remote SBA nodes on page 201 .

SMF node settings

Each SMF range includes a set of Node Settings and SMF NSSAI settings.

Node Settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple SMF instances may be deployed in the 5G network. Each SMF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
Name	The name uniquely identifies each SMF instance. You can accept the value provided by LoadCore or overwrite it with your own value.
PLMN MCC	The PLMN Mobile Country Code (MCC) for this SMF range.
PLMN MNC	The PLMN Mobile Network Code (MNC) for this SMF range.
HTTP Connections	The number of HTTP connections between two nodes.
Mapped SGW Range	Select the mapped serving gateway from the drop-down list.
PGW FQDN	Specify the PDN Gateway FQDN (Fully Qualified Domain Name).
Subscribe for ANF Events	Select the check box in order to enable this option.
UDP Buffer Size RX	The size in bytes of the receive buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 12582912
UDP Buffer Size TX	The size in bytes of the transmit buffers for UDP sockets: <ul style="list-style-type: none"> • minimum: 212992 • maximum: 134217728 • default: 2097152

SMF NSSAI

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

Setting	Description
<i>SMF NSSAI:</i>	
	Select the Add NSSAI button to add a NSSAI to your test configuration.
<i>SMF NSSI:</i>	
	Select the Delete NSSAI button to remove this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
DNNs	A DNN (Data Network Name) with which PDU sessions will be associated for this NSSAI. Select one or more DNNs from the drop-down list.

SMF N4 interface settings

N4 is the service-based interface through which a AMF instance interacts with UPF in a 5G network.

The following **Connectivity Settings** enable the necessary N4 connectivity and service interaction.

Setting	Description
<i>N4 Interface Settings:</i>	
Use Remote FTEID Allocation	When this option is enabled, SMF expects the UPF to allocate TEIDs. When it is disabled, the SMF allocates TEIDs.
Peer UPF	The IP address of the UPF node connected to SMF over the N4 interface.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

SMF Nsmf interface settings

Nsmf is the service-based interface through which a SMF instance makes its services available to other services in a 5G network.

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

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

Connectivity Settings	Description
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

SMF remote SBA nodes

- [AMF Connection Settings below](#)
- [UDM Connection Settings on the next page](#)
- [PCF Connection Settings on the next page](#)
- [NRF Connection Settings on page 203](#)

AMF Connection Settings

Setting	Description
<i>AMF Connectivity Settings:</i>	
Use SCP Node	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the check box to enable it. For more details, refer to Use SCP.</p>
Peer AMF Type	<p>Select one of the available options:</p> <ul style="list-style-type: none"> • Preset • Discover <p>More details below.</p>

The SMF can learn about the AMFs it serves, by selecting one of the following options for the Peer AMF type field:

- **Preset** - this option allows manually configuration of a peer AMF.

This option requires the configuration of the peer AMF, as follows:

Setting	Description
<i>AMF Peers:</i>	
	Select this button to add a peer AMF to your test configuration.
<i>AMF Peer:</i>	
	Select this button to delete the peer AMF from your test configuration.
Peer AMF	Select the peer AMF from the drop-down list.
Protocol	The protocol to use for Namf communications. It can be either HTTP or HTTPS.
Port	The AMF port number to use for Namf communications. The default is port 80, but you can choose a different port number.

- **Discover** - select this option to invoke the NF discovery service (it relies on the NRF to assign the correct Peer AMF during the handover procedure).

Refer to [NF Discovery service on page 304](#) for the steps required to use the discovery service.

UDM Connection Settings

To connect to the UDM node, the following configuration settings are required.

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM	Select the peer UDM using either of the following methods: <ul style="list-style-type: none"> • Select the IP address of the UDM node. This is the destination address of the UDM node to which the packets are sent over the Nudm interface. • Select Discover to invoke the NF discovery service. Refer to NF Discovery service on page 304 for the steps required to use the discovery service.
Protocol	The protocol to use for Nudm communications. It can be either HTTP or HTTPS.
Port	The UDM port number to use for Nudm communications. The default is port 80, but you can choose a different port number.

PCF Connection Settings

To connect to the PCF node, the following configuration settings are required.

Setting	Description
<i>PCF Connectivity Settings:</i>	

Setting	Description
Peer PCF	Select the peer PCF using either of the following methods: <ul style="list-style-type: none"> Select the IP address of the PCF node. This is the destination address of the PCF node to which the packets are sent over the NPCf interface. Select Discover to invoke the NF discovery service. Refer to NF Discovery service on page 304 for the steps required to use the discovery service.
Protocol	The protocol to use for Npcf communications. It can be either HTTP or HTTPS.
Port	The PCF port number to use for Npcf communications. The default is port 80, but you can choose a different port number.

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

For several SBA nodes, if SCP is selected in SCP Connection Settings, a new option will be available:

- **Use SCP Node**

If SCP is selected in SCP Connection Settings, the messages will be forwarded to SCP on all the interfaces where SCP is supported. If **Use SCP Node** check box option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which the **Use SCP Node** check box is enabled will be forwarded to the SCP.

NEF configuration settings



Network Exposure Function (NEF), located between the 5G core network and external third-party application functionaries, is responsible for managing the external open network data. All external applications that want to access the internal data of the 5G core must pass through the NEF.

IMPORTANT

NEF simulation is not supported when Technical Spec Version is **R15 September 2019**.

Topics:

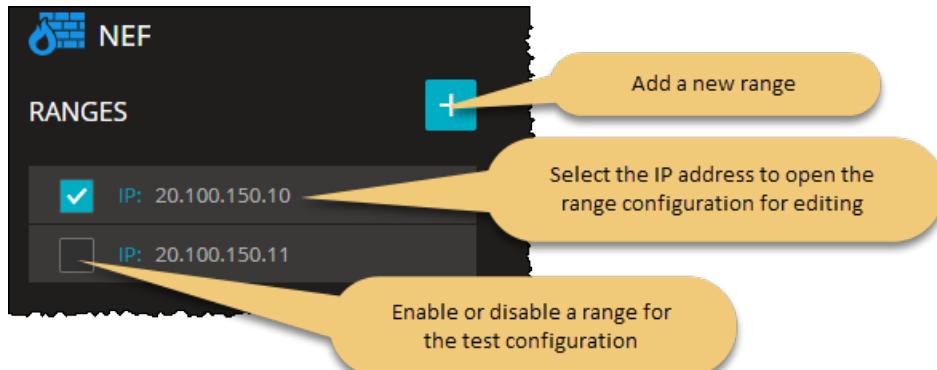
NEF Ranges panel	204
NEF Range panel	205
NEF Nnef interface settings	206
NEF Remote SBA Nodes	206

NEF Ranges panel

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

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

For example ...



NEF Range panel

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

- Select the **Delete Range** button to delete the selected NEF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the NEF range.

NEF range controls and settings

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

The following table describes the available **Range** configuration options for each NEF 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 NEF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the NEF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	The NEF Node Settings are described below (Node Settings below).
Nnef Interface Settings	Each NEF range requires the configuration of Nnefinterface settings, through which a NEF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in NEF Nnef interface settings on the next page .
Remote SBA Nodes	The remote SBA node settings are described in NEF Remote SBA Nodes on the next page .

Node Settings

The following table describes the available NEF Node Settings.

Setting	Description
Instance ID	Each NEF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.

NEF Nnef interface settings

Nnef is the service-based interface through which a NEF instance makes its services available to other services in a 5G network. The following **Connectivity Settings** enable the necessary Nnef 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 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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

NEF Remote SBA Nodes

IMPORTANT

If on the NEF node either UDM or UDR is selected but the other one is set to **None** (for example, UDM is set to a node but UDR is set to **None**), LoadCore shows this as a configuration error. When UDR is selected, the UDM needs to be set and vice versa.

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

PCF Connection Settings

To connect to the PCF node, the following configuration settings are required.

Setting	Description
<i>PCF Connectivity Settings:</i>	
Peer PCF	<p>Select the peer PCF using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the PCF node. This is the destination address of the PCF node to which the packets are sent over the NPCf interface. Select Discover to invoke the NF discovery service. Refer to NF Discovery service on page 304 for the steps required to use the discovery service.
Protocol	The protocol to use for Npcf communications. It can be either HTTP or HTTPS.
Port	The PCF port number to use for Npcf communications. The default is port 80, but you can choose a different port number.

UDM Connection Settings

To connect to the UDM node, the following configuration settings are required.

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM	Select either the IP address of an UDM from your test network or <i>None</i> if you are not using an UDM in your test configuration. The IP address is the destination address of the UDM node to which the packets are sent over the Nudm interface.

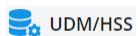
Setting	Description
Protocol	The protocol to use for Nudm communications. It can be either HTTP or HTTPS.
Port	The UDM port number to use for Nudm communications. The default is port 80, but you can choose a different port number.

UDR Connection Settings

To connect to the UDR node, the following configuration settings are required.

Setting	Description
<i>UDR Connectivity Settings:</i>	
Peer UDR	Select either the IP address of an UDR from your test network or <i>None</i> if you are not using an UDR in your test configuration. The IP address is the destination address of the UDR node to which the packets are sent over the Nudr interface.
Protocol	The protocol to use for Nudr communications. It can be either HTTP or HTTPS.
Port	The UDR port number to use for Nudr communications. The default is port 80, but you can choose a different port number.

UDM/HSS configuration settings



Unified Data Management (UDM) is the 5G core network service that is responsible for a number of functions, including the generation of AKA authentication credentials, user identification handling, access authorization, subscription management, among others. It makes its services available to other network functions through the Nudm service-based interface. Multiple instances of UDM may be deployed. A UDM Group ID refers to one or more UDM instances managing a specific set of SUPIs.

The Home Subscriber Server(HSS) is the master database for a given subscriber, acting as a central repository of information for network nodes. Subscriber related information held by the HSS includes user identification, security, location and subscription profile. The HSS is a functional element of LTE and IMS.

The configuration settings are described in the topics listed below.

Topics:

UDM/HSS Ranges panel	210
UDM/HSS Range panel	211
UDM/HSS node settings	211
UDM/HSS Nudm interface settings	215
UDM/HSS Remote SBA Nodes	216

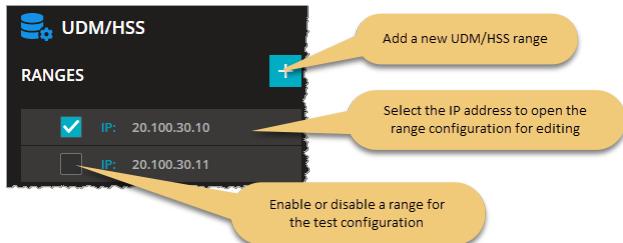
UDM/HSS Ranges panel

The **UDM/HSS Ranges** panel opens when you select the UDM/HSS node from the network topology window.

You can perform the following tasks from this panel:

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

For example ...



UDM/HSS Range panel

You add and select ranges from the UDM/HSS Ranges panel. When you select the IP address of a UDM, LoadCore opens the **Range** panel, from which you can:

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

UDM/HSS range controls and settings

Each range is identified by a unique IP address. You can add and delete ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each 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 UDM is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the UDM functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each UDM range requires the configuration of an associated set of Node Settings, which are described in UDM/HSS node settings below .
Nudm Interface Settings	Each UDM range requires the configuration of Nudm interface settings, through which a UDM instance enables connectivity and interaction with other functions in the 5G network. These settings are described in UDM/HSS Nudm interface settings on page 215 .
Remote SBA Nodes	The remote SBA node settings are described in UDM/HSS Remote SBA Nodes on page 216 .

UDM/HSS node settings

Each UDM/HSS range includes a set of Node Settings plus one or more associated Routing Indicators. Also, here you can configure the SDM notifications and the settings required for the S6a interface.

Node Settings

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

Setting	Description
Instance ID	The Instance ID uniquely identifies each UDM instance. You can accept the value provided by LoadCore or overwrite it with your own value.

Setting	Description
PLMN MCC	<p>The PLMN MCC for this UDM 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 UDM 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>
Home Network Private key	<p>The Home Network Private key that is used for subscriber privacy.</p> <p>The Subscription identifier de-concealing function (SIDF)—which is a service provided by the UDM—is responsible for de-concealing the SUPI from the SUCI. When the Home Network Public Key is used for encryption of the SUPI, the SIDF uses the Home Network Private Key that is securely stored in the home operator's network to decrypt the SUCI. The de-concealment takes place at the UDM. Access rights to the SIDF are defined such that only a network element of the home network is allowed to request SIDF.</p> <p>Note that one UDM can comprise several UDM instances. The Routing Indicator in the SUCI can be used to identify the specific UDM instance that is capable of serving a subscriber.</p> <p>About SUPI and SUCI ...</p> <p>The Subscription Permanent Identifier (SUPI) is a globally unique identifier allocated to each subscriber in the 5G System. The Subscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed SUPI.</p>
<p><i>Routing Indicators:</i> For details, refer to Routing Indicators.</p>	
<p><i>SDM Notifications:</i> For details, refer to SDM Notifications.</p>	
<p><i>HSS S6a:</i> You can enable or disable the S6a interface, as required by your test configuration.</p>	
Origin Host Prefix	Set the origin host prefix. Default value: host .

Setting	Description
Origin Realm	Set the origin realm. Default value: keysight.com .
Destination Host	Set the destination host prefix.
Destination Realm	Set the destination realm.
<i>Network Initiated Deregistration: You can enable or disable this option, as required by your test configuration.</i>	
Delay	Set the delay value.
Trigger	Describes what triggers the sending of the Network Deregistration message. Available options: <ul style="list-style-type: none">• Subscribe - AMF to UDM SDM subscription HTTP procedure• Update Location - MME to HSS Update Location Request Diameter procedure
Deregistration Reason	Select the deregistration reason from the drop-down list. Available options: <ul style="list-style-type: none">• UE INITIAL REGISTRATION• UE REGISTRATION AREA CHANGE• SUBSCRIPTION WITHDRAWN• 5GS TO EPS MOBILITY• 5GS TO EPS MOBILITY UE INITIAL REGISTRATION• REREGISTRATION REQUIRED
<i>Cancel Location: You can enable or disable this option, as required by your test configuration.</i>	
Delay	Set the delay value.

Routing Indicators

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.

You can add as many Routing Indicators as necessary to support your test objectives.

Setting	Description
	Select the Add Routing Indicator button to add a Routing Indicator for the UDM range.
	Select the Delete button to remove the routing indicator from the UDM range.

SDM Notifications

The UDM is a database-like Network Function(NF). It keeps information about the subscribers (users). The information about a subscriber is organized as a collection of resources corresponding to that user (*nssai*, *am-data*, *sm-data*, *smf-select-data* etc). A resource is a JSON object, containing sub-objects identified by a path.

When other Network Functions (NFs) register to UDM for a certain subscriber, they get some of those resources (for that specific user) and also ask the UDM to subscribe for changes to those resources (so for example, through a subscription operation, the AMF requests from the UDM a notification when *am-data* resource for this user changes).

Basically, through the SDM Notifications, UDM is delivering notifications to other interested NFs about changes to its resources.

The SDM Notifications defines a list of resources and the changes that occur for each of those resources

You can add as many SDM notification subscriptions as necessary to support your test objectives. To do this, select the **Add UDM Triggered SDM Notifications Table** button.

The following table describes the parameters that you need to configure for each SDM subscription.

Setting	Description
<i>SDM Subscription:</i>	
	Select the Delete Subscription button to remove this subscription from the SDM notifications.
Resource name	This represents the subscribed resource (entered as a string) for which notifications are triggered. Valid strings currently supported: <i>nssai</i> , <i>am-data</i> , <i>smf-select-data</i> , <i>sm-data</i> , <i>ue-context-in-smf-data</i> .
Notification trigger time (ms)	This represents the time interval (in milliseconds) from NF subscription (for that resource) after which that NF will start receiving notifications from UDM.
Change resource continuously	Select this option to apply the changes from the list continuously(start over again when reaching the end of the list). If this option is not selected, the notifications for the resource will stop when the last change in the list will happen, otherwise they will start from the beginning again.
<i>Resource changes:</i>	
	Select the Add change button to add new list of changes that will happen over time to the defined resource.
<i>Change Item</i>	
	Select the Delete Change Item to remove this list from your configuration.

Setting	Description
Change type	This represents the nature of the change: <ul style="list-style-type: none"> Add - new content was added to the resource. Replace - a certain content was replaced. Remove - a certain content was removed. Move - a certain content has been moved from one place to another.
Path in resource to change	The resource is a JSON object and it is comprised of multiple JSON sub-objects. This path describes which sub-object will be the target of the change (if left empty, it designated the resource object).
New JSON value	This represents the new JSON text value for the object identifier by the Path in resource to change . <p>IMPORTANT This field must have a valid JSON text value only if the Change type is set to Add or Replace.</p>
Trigger after previous notification change (ms)	This represents the time interval starting from the previous change notification, after which this notification should be delivered. The first notification would not use this value, it will be delivered using the value of Notification Trigger timer .
From source path (used for Move change type)	<p>NOTE This parameter is available only when Change type is set to Move.</p> <p>This represents the original path of the JSON object that has been moved.</p>

UDM/HSS Nudm interface settings

Nudm is the service-based interface through which a UDM instance makes its services available to other services in a 5G network.

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

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	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.

UDM/HSS Remote SBA Nodes

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not

Setting	Description
	using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

UDR configuration settings



Unified Data Repository (UDR) is the 5G core network service that maintains a repository of data that can be used by a number of 5G network functions. For example, the UDR may store subscription data that is used by the UDM and policy data that is used by the PCF. It makes its services available to other network functions through the Nudr service-based interface. Multiple instances of UDR may be deployed, with each instance storing specific data or providing service to a specific set of network function (NF) consumers.

The configuration settings are described in the topics listed below.

Topics:

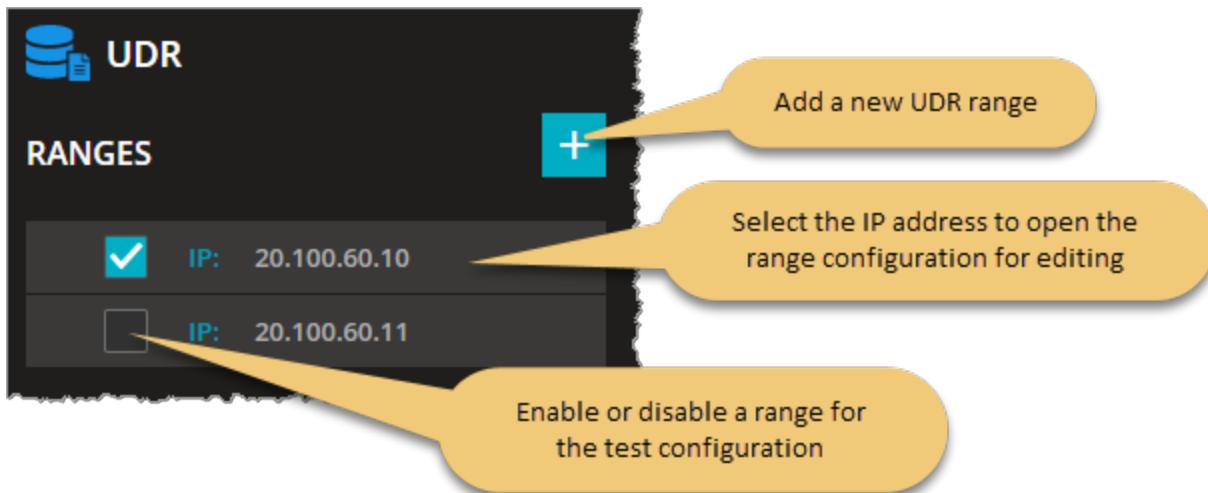
UDR Ranges panel	218
UDR Range panel	218
UDR Nudr interface settings	219
UDR Remote SBA Nodes	220

UDR Ranges panel

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

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

For example ...



UDR Range panel

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

- Select the **Delete Range** button to delete the selected UDR range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the UDR range.

UDR range controls and settings

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

The following table describes the available **Range** configuration options for each UDR 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 UDR is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the UDR functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Refer to the UDR Node Settings described below (Node Settings below).
Nudr Interface Settings	Each UDR range requires the configuration of Nudr interface settings, through which a UDR instance enables connectivity and interaction with other functions in the 5G network. These settings are described in UDR Nudr interface settings on page 358 .
Remote SBA Nodes	The remote SBA node settings are described in UDR Remote SBA Nodes on the next page .

Node Settings

The following table describes the available UDR Node Settings.

Setting	Description
Instance ID	Multiple UDR instances may be deployed in the 5G network, with each one storing specific data or providing service to a specific set of NF consumers. Each UDR instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.

UDR Nudr interface settings

Nudr is the service-based interface through which a UDR instance makes its services available to other services in a 5G network. The following **Connectivity Settings** enable the necessary Nudr connectivity and service interaction.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	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.

UDR Remote SBA Nodes

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.

Setting	Description
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

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 LoadCore, 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	221
CSCF N6 interface settings	222
CSCF Rx interface settings	223
CSCF UE routes settings	224
CSCF remote SBA nodes	224
Media Function Range panel	225

CSCF Range panel

When you select a CSCF's IP address from the **CSCF Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- Designate the range as a **Device Under Test**.
- 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>Range:</i>	
Device Under Test	Enable this option if your CSCF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the CSCF functionality (if it is selected in the Topology window).

Setting	Description
<i>Range Settings:</i>	
N6 Interface Settings	The CSCF range requires the configuration of N6 interface settings (this interface is used for SIP). These settings are described in CSCF N6 interface settings below .
Rx Interface Settings	The CSCF range requires the configuration of Rx interface settings (this interface is used for Diameter). These settings are described in CSCF Rx interface settings on the facing page .
UE Routes Settings	These settings are described in CSCF UE routes settings on page 224 .
Remote SBA Nodes	The remote SBA node settings are described in CSCF remote SBA nodes on page 224 .

CSCF N6 interface settings

N6 is the service-based interface through which a CSFC instance makes its services available to other services in a 5G network.

Interface Settings

The following settings are required to enable N6 interface transmission.

Interface setting	Description
Domain	Set the domain served by the SIP proxy.
Port	Set the SIP port number for the proxy.
Support TLS Transport	Select this check box to enable TLS transport.

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

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

Connectivity Settings	Description
Increment	Gateway Address).
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.
Inner VLAN	<p>IMPORTANT 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.

CSCF Rx interface settings

Rx is the service-based interface through which a P-CSCF instance makes its services available to other services in a 5G network.

Interface Settings

The following settings are required to enable message transmission between the P-CSCF and PCRF.

Interface setting	Description
Hostname	Set the hostname.
Realm	Set the realm. Default value: keysight.com .

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

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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).
Outer VLAN	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.

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

CSCF UE routes settings

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

Settings	Description
<i>UE Routes Config:</i>	
	Select this button to add a new route to a specific UE range.
<i>UE Routes Config:</i>	
	Select this button to remove the route to the UE range.
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.

CSCF remote SBA nodes

PCRF Connection Settings

To connect to the PCRF node, the following configuration settings are required.

Setting	Description
<i>PCRF Connectivity Settings:</i>	
Peer PCRF	Select the IP address of the PCRF node.

Media Function Range panel

When you select a Media Function 's IP address from the **Media Function Ranges** panel, LoadCore opens the **Range** panel, from which you can configure the node and 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.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

UPF/PGW-U configuration settings



UPF/PGW-U

User Plane Function (UPF) is one of the fundamental components of the 5G core architecture. It is the interconnection point between the mobile infrastructure and the Data Networks (DN) and, as such, it is responsible for encapsulating and decapsulating the GPRS Tunneling Protocol for the user plane (GTP-U). Among its key responsibilities are packet routing and forwarding, packet inspection and QoS handling, user plane lawful intercept, and providing the mobility anchor for intra-RAT and inter-RAT handovers.

UPF interacts with the DN over the N6 reference point, with the RAN over the N3 reference point, and with the SMF over the N4 reference point. In addition, the N9 reference point is used for interactions among UPFs, such as an I-UPF and the PDU session anchor UPF.

PGW-U, introduced in 3GPP Release 14 as part of the Control and User Plane Separation strategy (CUPS), handles the user plane forwarding responsibilities in 4G networks.

The configuration settings are described in the topics listed below.

Topics:

UPF/PGW-U Ranges panel	227
UPF/PGW-U Range panel	227
UPF N3 interface settings	228
UPF N4 interface settings	229
UPF N6 interface settings	231
UPF N9 interface settings	231

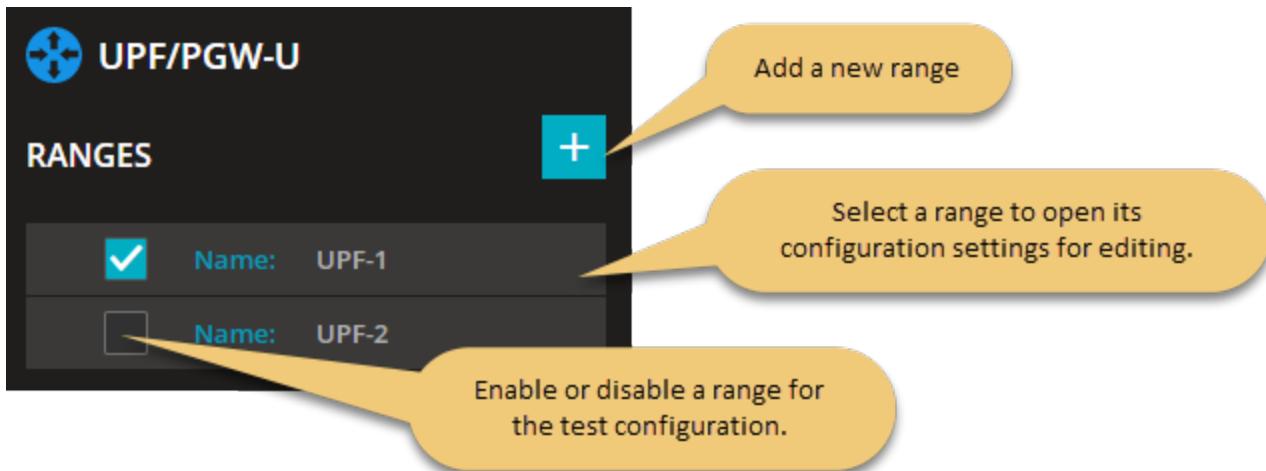
UPF/PGW-U Ranges panel

The **UPF/PGW-U Ranges** panel opens when you select the UPF/PGW-U node from the network topology window.

You can perform the following tasks from this 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 ...



UPF/PGW-U Range panel

You add and select UPF ranges from the UPF/PGW-U Ranges panel. When you select a UPF range **Name**, LoadCore opens the **Range** panel, from which you can:

- Delete the UPF range from the test configuration.
- Designate the range as a **Device Under Test**.
- 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.
Device Under Test	Enable this option if your UPF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the UPF functionality (if it is selected in the Topology window).

Setting	Description
Name	The name of the UPF range. You can accept the name provided by the LoadCore, 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 below .
N4 Interface Settings	N4 is the interface between the SMF and the UPF. These interface settings are described in UPF N4 interface settings on the facing page .
N6 Interface Settings	N6 is the interface between the DN and the UPF. These interface settings are described in UPF N9 interface settings on page 231 .
N9 Interface Settings	N9 is the interface between two UPFs. These interface settings are described in UPF N9 interface settings on page 231 .

UPF N3 interface settings

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

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

Setting	Description
<i>N3 Interface Settings:</i>	
Network Instance	The network domain that will be used in the Network Instance information element (IE) in messages sent on this interface. The UPF uses the Network Instance to determine the IP network to use when transferring traffic over the N3 interface.
<i>Network Instance:</i>	
	Select the Add value button to add a network instance to your test configuration.
	Select the Delete button to remove the network instance from your test configuration.
Network Instance Format	Select the encoding format for the network instance: string or label-list.

Connectivity Settings

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

UPF N4 interface settings

The UPF receives user traffic information from the SMF over the N4 interface. N4—which employs the Packet Forwarding Control Protocol (PFCP)—is the control plane interface between the UPF and the

SMF. PFCP sessions established with the UPF define how packets are identified, forwarded, processed, marked, and reported (using PDRs, FARs, BARs, QERs, and URRs).

The following configuration settings are required by each UPF N4 range.

Setting	Description
<i>N4 Interface Settings:</i>	
Supports FTEID Allocation	When this option is enabled, the UPF allocates TEIDs. When it is disabled, the UPF expects the SMF to allocate TEIDs.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
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>	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	<p>IMPORTANT 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>

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

UPF N6 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** are required by each UPF N6 range.

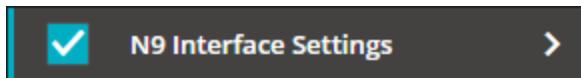
NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

UPF N9 interface settings

N9 is the interface between two UPFs in a 5G network: for example an I-UPF and the UPF session anchor. An I-UPF performs a relay function, while the session anchor terminates the protocols (such as GTP) used on that interface.

You can enable or disable the N9 Interface Settings, as required by your test configuration. For example:



The following **Interface Settings** are available only if the **N9 Interface Settings** check-box is selected.

Interface Settings	Description
Network Instance	The network domain that will be used in the Network Instance information element (IE) in messages sent on this interface. The UPF uses the Network Instance to determine the IP network to use when transferring traffic over the N9 interface.
<i>Add Network Instance:</i>	
	Select the Add value button to add a network instance to your test configuration.
	Select the Delete button to remove the network instance from your test configuration.
Network Instance Format	Select the encoding format for the network instance: string or label-list.

Connectivity Settings

The following **Connectivity Settings** enable the necessary N9 connectivity between UPF nodes.

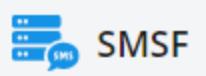
NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

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

SMSF configuration settings



Short Message Service Function (SMSF) is the 5G core network service that supports the transfer of SMS over NAS. In this capacity, the SMSF will conduct subscription checking and perform a relay function between the device and the SMSC (Short Message Service Centre), through interaction with the AMF (Core Access and Mobility Management Function).

The configuration settings are described in the topics listed below.

Topics:

SMSF Ranges panel	234
SMSF Range panel	235
SMSF node settings	235
SMSF Nsmsf interface settings	236
SMSF Remote SBA Nodes	237

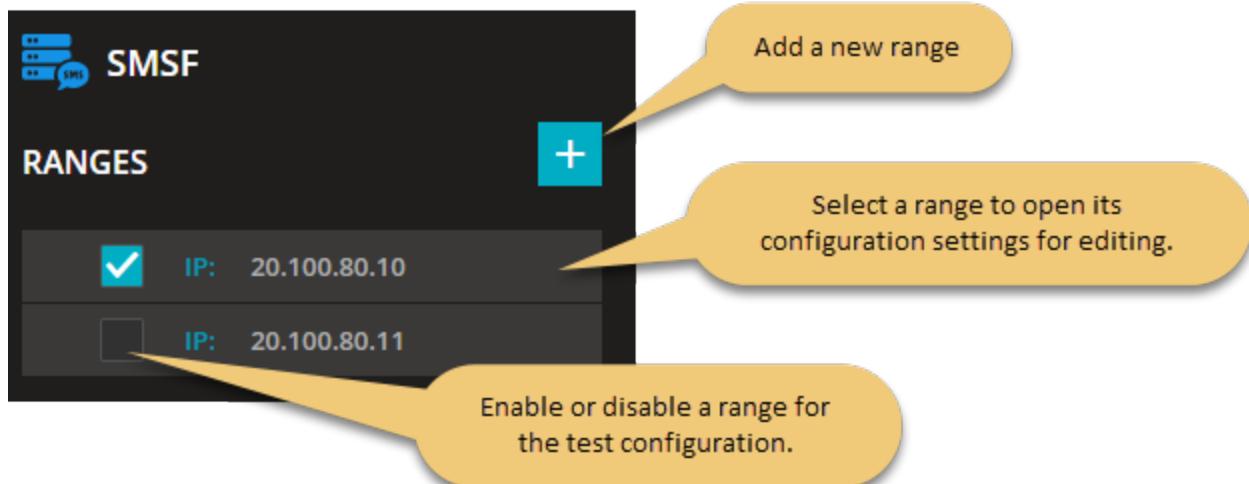
SMSF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



SMSF Range panel

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

- Delete the selected SMSF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the SMSF range.

SMSF range controls and settings

Each SMSF range is identified by a unique IP address. You can add and delete SMSF ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each SMSF 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 SMSF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the SMSF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	These settings are described in SMSF node settings below .
Nausf Interface Settings	Each SMSF range requires the configuration of Nsmsf interface settings, through which a SMSF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in SMSF Nsmsf interface settings on the next page .
Remote SBA Nodes	These settings are described in SMSF Remote SBA Nodes on page 237 .

In order to configure the SMSF node to perform MT-SMS, it is required that on **UE Range Settings > SMS Configurations > SMSF Configuration**, to set SMS Mode to **MT-SMS**. When this is selected, and the node is enabled, the settings from **Mobile Settings** will be translated to the SMSF node as parameters for MT-SMS.

NOTE

The LoadCore AMF does not support SMS over HTTP2, so an AMF set as DUT is required in order to trigger MO-SMS over HTTP2.

SMSF node settings

Each SMSF instance (that is, each range) requires the configuration of the following node settings.

Setting	Description
Instance ID	The Instance ID uniquely identifies each SMSF instance. You can accept the value provided by LoadCore or replace it with your own value.

SMSF Nsmsf interface settings

Nsmsf is the service-based interface through which a SMSF instance makes its services available to other services in a 5G network.

The following **Connectivity Settings** enable the necessary Nsmsf 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 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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

SMSF Remote SBA Nodes

Peer AMF

To connect to one or more AMF nodes, the following configuration settings are required.

Setting	Description
Peer AMF	Select the peer AMF from the drop-down list, which provides these options: <ul style="list-style-type: none"> <i>Select All</i>: Select this option to establish connections to all of the AMF nodes configured in the test. <i>specific AMF</i>: Select one or more of the individual AMF nodes from this list to establish connects with only those nodes.

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

5G-EIR configuration settings



Equipment Identity Register (5G-EIR) is a network function of 5G Core which is used to check the status of PEI(Permanent Equipment Identifier) (e.g., PEI blacklist status). It provides services for authentication and arbitrary device change processing to prevent unauthorized use of devices depending on the PEI status on 5G Core.

Topics:

5G-EIR Ranges panel	238
5G-EIR Range panel	238
5G-EIR node settings	239
5G-EIR N5g-eir interface settings	239
5G-EIR Remote SBA Nodes	240

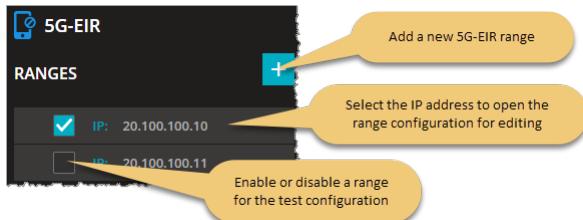
5G-EIR Ranges panel

The **5G-EIR Ranges** panel opens when you select the 5G-EIR node from the network topology window. Each 5G-EIR range is identified by a unique IP address that you configure.

You can perform the following tasks from this panel:

- Add a new 5G-EIR range to your test configuration.
- Open a 5G-EIR range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



5G-EIR Range panel

When you select the IP address of a 5G-EIR range from the 5G-EIR Ranges panel, LoadCore opens the **Range** panel for that selected 5G-EIR. From that Range panel you can:

- Delete the selected 5G-EIR range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the 5G-EIR range.

5G-EIR range controls and settings

Each 5G-EIR range is identified by a unique IP address. You can add and delete ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each 5G-EIR 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 5G-EIR is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the 5G-EIR functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each 5G-EIR range requires the configuration of an associated set of Node Settings, which are described in 5G-EIR node settings below .
N5g-eirInterface Settings	Each 5G-EIR range requires the configuration of N5g-eir interface settings, through which a 5G-EIR instance enables connectivity and interaction with other functions in the 5G network. These settings are described in 5G-EIR N5g-eir interface settings below .
Remote SBA Nodes	The remote SBA node settings are described in 5G-EIR Remote SBA Nodes on the next page .

5G-EIR node settings

Each 5G-EIR range includes a set of Node Settings.

Node Settings

Each 5G-EIR instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple 5G-EIR instances may be deployed in the 5G network. Each 5G-EIR instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.

5G-EIR N5g-eir interface settings

N5g-eir is a service-based interface exhibited by 5G-EIR (5G-Equipment Identity Register) which is an optional network function that checks the status of Equipment's identity (e.g. to check that it has not been blacklisted).

The following **Connectivity Settings** enable the necessary N5g-eir connectivity and service interaction.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
<i>Outer VLAN</i>	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
<i>Inner VLAN</i>	<p>IMPORTANT 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.

5G-EIR Remote SBA Nodes

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can

Setting	Description
	choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

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:

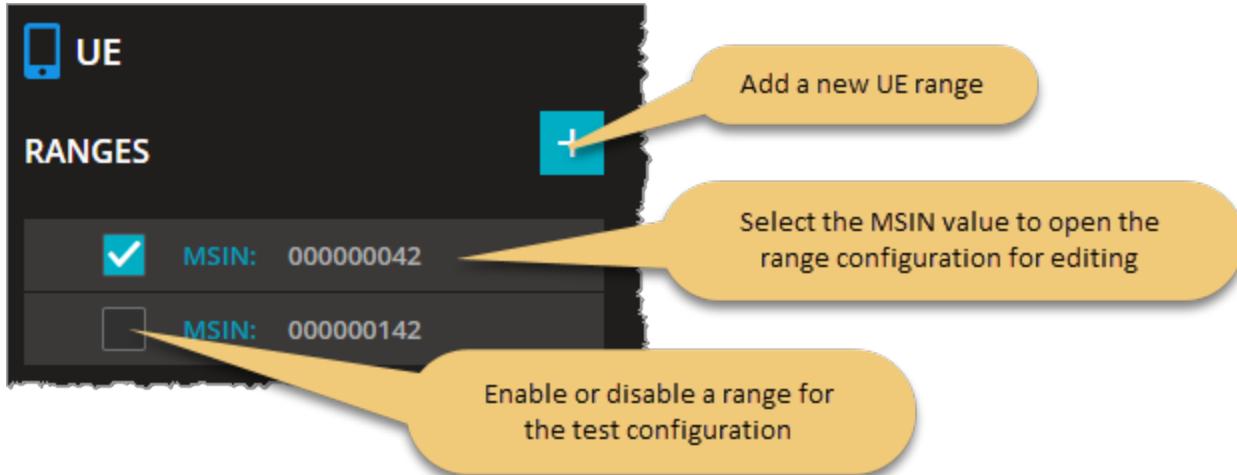
UE Ranges panel	243
UE Range panel	244
Range Settings	246
UE Identification settings	247
UE Security settings	247
UE Settings settings	249
UE Shared Data IDs	253
UE Subscribed AMBR settings	253
Service Area Restriction settings	253
Forbidden Areas	255
DNNs Config	256
Notifications	257
SMS Configuration	258
Equipment Status	259
Network Slicing settings	260
UE NSSAI settings	261
UDM Default NSSAI settings	262
UDM SNSSAI Mappings	262
UDR SNSSAI Settings	263

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

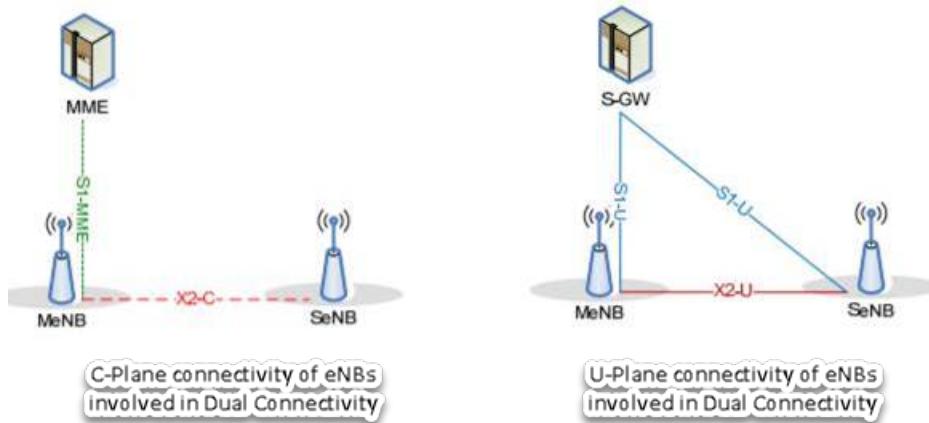
When you select an MSIN from the UE **Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- Delete the UE range from the test configuration.
- Configure the *Range Count*.
- Select the *Parent NG-RAN* for the UE range.
- Access the detailed UE configuration settings (Range Settings, Network Slicing, Objectives).

UE range controls and settings

LoadCore has now support for Option3x, 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 LoadCore 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 in NSA topology** [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.
- Currently Option 3x support is implemented only on S1-MME interface (there is no Option3x support implemented for full 4G core).

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	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 available only IF the parent node is an eNodeB. Select the secondary node from the drop-down list.

Detailed UE configuration settings

The Range panel also provides links to the detailed configuration settings:

- [Range Settings on the next page](#)
- [Network Slicing settings on page 260](#)
- [Objectives on page 264](#)

Range Settings

For each range that you add (in the [UE Ranges panel on page 243](#)), you configure the settings from the **Range** panel ([UE Range panel on page 244](#)).

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

UE Identification settings	247
UE Security settings	247
UE Settings settings	249
UE Shared Data IDs	253
UE Subscribed AMBR settings	253
Service Area Restriction settings	253
Forbidden Areas	255
DNNs Config	256
Notifications	257
SMS Configuration	258
Equipment Status	259

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 SV	The IMEI SV value that will be assigned to the first simulated UE in the range.
IMEI SV increment	The value to use for incrementing the IMEISV values for each of the UEs in the range.
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	<p>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.</p> <p>You can accept the value generated by LoadCore, or enter of a K value of your</p>

Setting	Description												
	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	<p>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.</p> <p>You can accept the value generated by LoadCore, or enter of an OP value of your own choosing.</p>												
OPc	<p>The OPc value is derived from the subscriber key K and the operator dependent value OP. You can accept the value generated by LoadCore, or enter of an OP value of your own choosing.</p>												
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.												
RAND	<p>A hexadecimal number that represents the 128-bit random challenge.</p> <p>You can accept the value generated by LoadCore, or enter of a RAND value of your own choosing.</p>												
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>												
SUCI Protection Scheme	<p>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:</p> <table border="1"> <thead> <tr> <th>Scheme</th> <th>Identifier</th> <th>Size of the scheme output</th> </tr> </thead> <tbody> <tr> <td>null-scheme</td> <td>0x0</td> <td>Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)</td> </tr> <tr> <td>Profile-A</td> <td>0x1</td> <td>Total of 256-bit public key, 64-bit MAC, and size of input</td> </tr> <tr> <td>Profile-B</td> <td>0x2</td> <td>Total of 264-bit public key, 64-bit MAC, and size of input.</td> </tr> </tbody> </table>	Scheme	Identifier	Size of the scheme output	null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)	Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input	Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.
Scheme	Identifier	Size of the scheme output											
null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)											
Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input											
Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.											
Home Network	The home network public key that will be use for concealing the SUPI. The USIM												

Setting	Description
Public Key	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	The Routing Indicator that is used in the construction of the SUCI. The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.

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>	
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.
Switch Off Deregistration	When this option is enabled, the Deregistration Request messages will use a deregistration type of <i>Switch-off</i> . (When the Deregistration type is switch-off, the AMF does not send the Deregistration Accept message to the UE.)
PDU Session Release Before Deregistration	When this option is enabled, the UE will release PDU sessions before deregistration.
Enable Passthrough	Select this option to enable passthrough. When passthrough is enabled, on the passthrough interface, the LoadCore waits for packets. Once received, the packets are encapsulated and transferred via N3 to the other side of the network.
Register with GUTI	When the Primary Objective type is Subscribers Per Second, you can enable this option to trigger a Registration Request with the type of user identity set to 5G-GUTI.

Setting	Description
	When this option is not enabled, the type of user identity in the Registration Request will be SUCI (Subscription Concealed Identifier).
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>
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.
Support SMS	<p>When this is selected, a flag will be added in the Registration message that will allow UEs to advertise that they support SMS feature).</p> <p>NOTE This feature is available on N1-N2 interface but the LoadCore AMF does not support SMS, so the AMF needs to be set as DUT.</p>
IP Address Increment	<p>The value by which the UE IP addresses will be incremented. This refers to all IP addresses assigned to the UE connected to multiple DNNs.</p> <p>When a UE is connected to multiple DNNs, it will have multiple IPs (at least one for each DNN connection). You configure the mapping between DNNs and UE IPs using the UE Range Settings DNNs Config panel (as described in DNNs Config on page 256).</p>

Setting	Description
SSC Mode	<p>The Session and Service Continuity (SSC) Mode for the PDU Sessions that UEs in this range will initiate.</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, IPv4v6) is not preserved in this mode when the PDU Session Anchor changes. <p>SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session.</p>
RAT Restrictions	UE Mobility Restrictions include RAT restrictions, which define the 3GPP Radio Access Technologies (one or more) that a UE is not allowed to access in a PLMN. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual.
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>
Active Time (s)	The subscribed Active Time for Power Saving Mode (PSM) UEs.
Allow MICO Mode	This option, when selected, indicates that the UEs in the range prefer Mobile Initiated Connection Only (MICO) mode during Initial Registration and Registration Update procedures.
Delay Before PDU Session Creation (ms)	The time that will elapse before the UEs in this range begin creating PDU sessions.
Delay Before Deregister (ms)	The time that will elapse before the UEs in this range begin the deregistration process.
Delay Before Handover Notify (ms)	This parameter is used to delay the handover procedure completion, in order to send multiple packets on the Indirect Data Forwarding Tunnels.
Delay Before Indirect Forwarding Cleanup (ms)	The time that will elapse before indirect forwarding cleanup.

Setting	Description
Send Native GUTI During IRAT Mobility Registration	Select this check box 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.
Check AUTN	<p>By default, this option is not selected.</p> <p>When the check box is selected, 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>
<i>Access and Mobility Policy:</i>	
Subscription Categories	Select the desired Subscription Category for this range of UEs. <i>Subscriber Category</i> 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).
Location Reporting	Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).
Reporting Type	Select the value from the drop-down list. The available options are: <ul style="list-style-type: none"> Direct - If the test timeline is long enough, the AMF generates n <code>LocationReportingControl</code> 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 <code>LocationReportingControl</code> message to the NG-RAN.
Interval Between Requests (seconds)	Set the time interval between requests.
Number of Repeats	Set the number of repeats.

Setting	Description
Start Time (seconds)	The number of seconds after successful attach when the AMF sends a LocationReportingControl message (event-type: change-of-serv-cell).
Stop Time (Seconds)	The number of seconds since the Start Time when the AMF sends LocationReportingControl message (event-type: stop-change-serving-cell).

UE Shared Data IDs

You use the **Shared Data ID** panel to create a list of shared-data-ids. These IDs are used to request the shared-data resources from the UDM.

A UE subscription may contain both individual subscription data and shared subscription data (subscription data that is shared by multiple UEs). These shared data are identified by Shared Data IDs that are listed in the UE individual data.

Use the **Add ID** button to add additional IDs to the list, and the **Delete ID** button to removed IDs from the list.

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 Session-AMBR value for this range of UEs.
Subscribed AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Subscribed AMBR Downlink	The subscribed downlink Session-AMBR value for this range of UEs.
Subscribed AMBR Downlink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.

Service Area Restriction settings

A UE subscription may contain service area restrictions, which place limits on the areas in which the UE may initiate communication with the network. A Service Area Restriction definition consists of either a list of allowed Tracking Area Identities (TAIs) or a list of non-allowed TAIs and, optionally, specifies the maximum number of allowed TAIs.

You use the settings described below to configure service area restrictions for a UE range (these configuration settings are also made available on the UDM). You can add and delete service area restriction Areas for the UE range as needed to meet your test requirements.

Service Area Restrictions

Setting	Description
Restriction Type	<p>The type of restriction to use for this range of UEs. It is either Not Allowed Areas or Allowed Areas.</p> <p>The list of allowed TAIs indicates the TAIs where the UE is allowed to be registered, and the list of non-allowed TAIs indicates the TAIs where the UE is not allowed to be registered.</p> <p>A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).</p>
Max No. of TAs	The maximum number of allowed TAIs for this UE range.

Areas

Each Service Area Restriction specifies one or more Areas (Allowed or Not Allowed Areas), each of which contains a list of TACs. You can add and delete areas from the Service Area Restrictions settings as needed to meet your test requirements.

Setting	Description
<i>Areas:</i>	
	Select the Add Area button to add a new restriction area to your configuration.
<i>Area:</i>	
	Select the Delete Area button to remove the restriction area from your configuration.
Area Codes	Each Area that you configure is identified by an Area Code, which is an operator-specific string value.
<i>TACs:</i>	
	<p>Select the Add TAC button to add a new TAC to your configuration.</p> <p>Each Area that you add to a UE range's Service Area Restriction contains a list of one or more TACs.</p> <p>A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is</p>

Setting	Description
	the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).
	Select the Delete button to remove the tracking area code from your configuration.

Forbidden Areas

A UE subscription may include a list of Forbidden Areas. In a Forbidden Area, the UE is not permitted to initiate any communication with the network.

You use the settings described below to configure forbidden areas for a UE range (these configuration settings are also made available on the UDM). You can add and delete Forbidden Areas for the UE range as needed to meet your test requirements.

Setting	Description
<i>Forbidden Area:</i>	
	Select the Delete Forbidden Area button to remove this area from your configuration.
Area Codes	Each Area that you configure is identified by an Area Code, which is an operator-specific string value.
<i>TACs:</i>	
	Select the Delete button to remove this TAC from your configuration.
TAC	Each Area that you add to a UE range's Forbidden Area contains a list of one or more TACs. A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).

DNNs Config

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

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

Setting	Description
<i>DNNs Config:</i>	
	From the panel, you can select a DNN Config for editing and also add addition DNN configurations. Select the Add DNNs Config button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the Delete DNN Config button to delete this DNN config from your test configuration.
DNN	Select one of the previously-defined DNNs from the drop-down list. (The DNNs are configured in the Global settings. Refer to DNN configuration settings on page 86 for a description of the settings.)
Local IPv4 Address	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). It is used only when LoadCore simulates the SMF. It is mostly used in tests when LoadCore simulates the SMF, but in cases with DUT it is recommended to put an IP from the range configured on SMF.
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 IPv6 Address	The IPv6 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). It is used only when LoadCore simulates the SMF. It is mostly used in tests when LoadCore simulates the SMF, but in cases with DUT it is recommended to put an IP from the range configured on SMF.
Local IPv6 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.
Ethernet Device Information	Allows adding multiple ethernet devices per DNN with PDU type Ethernet. NOTE This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.
Ethernet PDU config	For each ethernet device the MAC Address, IP Address, outer VLAN and inner VLAN can be configured.
Enable TSN	This feature is available only for spec version newer (including) Release 16 and Ethernet PDU type sessions.

Setting	Description
	<p>NOTE This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</p>
DS-TT Ethernet Port MAC Address	The device-side TSN translator port MAC address.
Configure S-NSSAI:	<p><i>When this checkbox is selected, you can configure which slice (S-NSSAI) to be send in PDU Session Establishment messages. If the checkbox is not selected, the first slice in Allowed NSSAI list is used in PDU Session Establishment message.</i></p> <p>NOTE <i>This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</i></p>
S-NSSAI	This list contains all the slices defined for the selected UE range. Select from the drop-down list the slice to be used in PDU Session Establishment.
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 checkbox 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 checkbox 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>

Notifications

Each UE range in the SBA topology has a set of **Notifications** values that configure Unified Data Repository (UDR) notifications for the range.

The UDR stores policy data that is used by the network service consumers (PCF, UDM, and NEF). Among the functionalities supported by the UDR is subscriptions to notification and the notification of subscribed data changes.

Setting	Description
<i>UDR Notifications:</i>	
Delay in milliseconds	The delay in milliseconds between Policy Data Subscriptions and Policy Data Change Notification.
<i>Policy Data:</i>	
Enable notification	Enable subscription to policy data notifications for the UE range.
SM Policy Data	Paste your policy data JSON file into the field.

Setting	Description
json	
<i>Application Data:</i>	
Enable notification	Enable subscription to application data notifications for the UE range.
Application Data json	Paste your application data JSON file into the field.

SMS Configuration

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

Setting	Description
<i>Mobile Settings:</i>	
Service Center Address	The service center address used by the UE range for SMS messaging.
Type of Number	<p>The type of number can be one of the following:</p> <ul style="list-style-type: none"> • Unknown • International number • National number • Network specific number • Subscriber number • Alphanumeric • Abbreviated number • Reserved number
Numbering Plan Identification	<p>The numbering plan identification can be one of the following:</p> <ul style="list-style-type: none"> • Unknown • ISDN • Data numbering plan • Telex numbering plan • National numbering plan • Private numbering plan • ERMES numbering plan • Reserved 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.

Setting	Description
Mobile Terminate SMS Delay (s)	The time in seconds to wait, after the UE registers, for the AMF or SMF to initiate an MT SMS.
<i>SMS Configuration:</i>	
SMS Mode	Select an option from the drop-down list: <ul style="list-style-type: none"> • SMS-MO: Mobile Originated. The UE range originates (sends) SMS messages. • SMS-MT: Mobile Terminated. The UE range waits for delivery of SMS messages.

Equipment Status

The Equipment Status that lets you configure blocked or greylisted ranges of UEs using the IMEI.

The following table describes the UE **Equipment Status** settings.

Setting	Description
<i>Blocked Subscribers:</i>	
	Select the Add Blocked Subscribers button to add a new range of blocked IMEIs.
	Select the Delete Blocked Subscribers button to delete this range of blocked IMEIs from your test configuration.
Start IMEI	Set the first IMEI of the blocked subscribers range.
End IMEI	Set the last IMEI of the blocked subscribers range.
Step	Set the step for the blocked subscribers range.
<i>Greylisted Subscribers:</i>	
	Select the Add Greylisted Subscribers button to add a new range of greylisted IMEIs.
	Select the Delete Greylisted Subscribers button to delete this range of greylisted IMEIs from your test configuration.
Start IMEI	Set the first IMEI of the greylisted subscribers range.
End IMEI	Set the last IMEI of the greylisted subscribers range.
Step	Set the step for the greylisted subscribers range.

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	261
UDM Default NSSAI settings	262
UDM SNSSAI Mappings	262
UDR SNSSAI Settings	263

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 border="1"> <thead> <tr> <th>SST</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>eMBB</td> <td>1</td> </tr> <tr> <td>URLCC</td> <td>2</td> </tr> <tr> <td>MIoT</td> <td>3</td> </tr> </tbody> </table>	SST	Value	eMBB	1	URLCC	2	MIoT	3
SST	Value								
eMBB	1								
URLCC	2								
MIoT	3								
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.								
Mapped SST	The Mapped configured Slice/Service Type (SST) value for this S-NSSAI.								
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this S-NSSAI.								

UDM Default NSSAI settings

You can add and delete UDM Default SNSSAI settings as required to meet your test objectives.

A UE Registration Request will include the Default Configured NSSAI Indication if the UE is using a Default Configured NSSAI. The Default Configured NSSAI, when configured in the UE, is used by the UE in a Serving PLMN only if the UE has no Configured NSSAI for the Serving PLMN.

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

Setting	Description
<i>UDM Default NSSAI:</i>	
	Select the Add UDM Default NSSAI button to add the default NSSAI to your test configuration.
<i>UDM Default NSSAI settings:</i>	
	Select the Delete UDM Default NSSAI button to delete this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this S-NSSAI.
Mapped SST	The default Mapped configure Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The default 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.

Setting	Description
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 one or more DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .

UDR SNSSAI Settings

The following table describes the UE **UDR SNSSAI** settings.

Setting	Description
<i>UDR SNSSAI Settings:</i>	
	Select the Add SNSSAI Settings button to add the SNSSAI settings to your test configuration.
<i>UDR Settings:</i>	
	Select the Delete SNSSAI Settings button to delete this SNSSAI settings configuration from your test configuration.
SST	The Slice/Service Type (SST) value
SD	The Slice Differentiator (SD) value for this SNSSAI. 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 Slice/Service Type (SST) value for this SNSSAI.
Mapped SD	The Mapped Slice Differentiator (SD) value for this SNSSAI.
DNNS	A DNN (Data Network Name) with which PDU sessions will be associated for this SNSSAI. Select one or more DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .

Objectives

In a LoadCore 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	265
About primary objectives	266
Primary Control Plane Objective	268
Secondary Control Plane Objective	270
User Plane Objectives	279
Stateless UDP Traffic	280
Data Traffic	281
Voice Traffic	284
Video OTT Traffic	287
DNS Client Traffic	290
Predefined Applications Traffic	293

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 on the next page](#)
- [Primary Control Plane Objective on page 268](#)
- [Secondary Control Plane Objective on page 270](#)

About primary objectives

In the current LoadCore 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 below](#)
- [Subscribers Per Second on the facing page](#)

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
Sustain time	Traffic and/or secondary objectives are executed
Ramp down	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 (`<number_of_subscribers_in_the_range> / <RampUpRate>`). If the ramp up rate cannot be maintained, ramp up will last longer.
- During the sustain time phase, only secondary objectives are running.
- If configured, uplink traffic will start after the ramp up stage is complete.
- Subscribers will accept any downlink traffic once they are attached (registered and PDU session established).
- The duration of ramp down is not directly configurable. The ramp down time is automatically computed from the total number of subscriber in the range divided by the configured Ramp-up Rate (`<number_of_subscribers_in_the_range> / <RampUpRate>`). If the ramp down rate cannot be maintained, ramp down will last longer.

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>	$2000 / 1000 = 20\text{s}$ for subscribers to deregister
<i>Rate in ramp down time:</i>	1000 deregistrations per second

Subscribers Per Second

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

Such a test will give the following results.

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

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.
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 test in the Global Settings. Refer to DNNs panel on page 85 for more information.</p>
<i>Subscribers Per Second:</i>	
Hold Time	The number of milliseconds 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

Parameter	Description
	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.
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 test in the Global Settings. Refer to DNNs panel on page 85 for more information.</p>

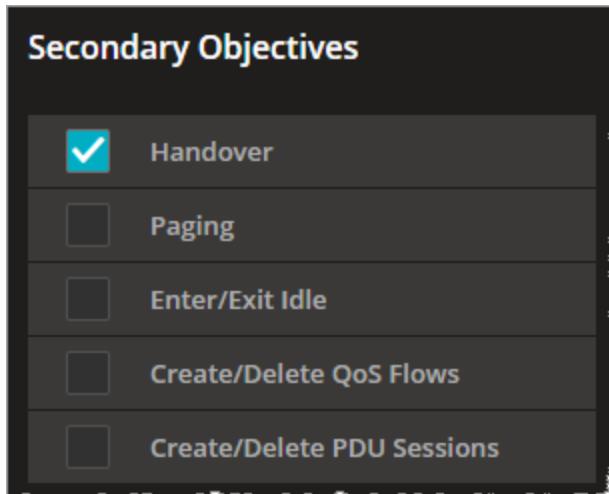
Secondary Control Plane Objective

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 on the facing page](#)
- [Paging on page 273](#)
- [Enter/Exit Idle on page 274](#)
- [Create/Delete QoS Flows on page 275](#)
- [Create/Delete PDU Sessions on page 277](#)

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 on page 244](#)). The UEs then traverse the NG-RANs that you configure (the *Visited NG-RAN* list).

Handover notes

- Xn handover and N2 handover are supported.
- Xn handover is executed when the AMF serving the UE can reach the target RAN (T-RAN) and an Xn link is configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.

N2 handover scenarios

For N2 handover there are the following scenarios:

Scenario	Description
N2 handover with AMF change and Direct Forwarding	This scenario is executed when the AMF serving the UE cannot reach the target RAN (T-RAN) and an Xn link is configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.
N2 handover with AMF change and Indirect Forwarding	This scenario is executed when the AMF serving the UE cannot reach the target RAN (T-RAN) and an Xn link is not configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.
N2 handover without AMF change and Indirect Forwarding	This scenario is executed when the AMF serving the UE can reach the target RAN (T-RAN) but an Xn link is not configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.
N2 handover without AMF change and Direct Forwarding	This scenario is executed when the AMF serving the UE can reach the target RAN (T-RAN), ForceN2 option is set and Xn link is configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.

Option3x handover scenarios

For Option3x handover there is support for the following:

- X2 Handover support between eNodeBs – only S1 signaling is visible
- Option 3x handovers support:
 - Inter-Master Node handover with/without Secondary Node change (X2 handover between 2 eNodeBs that have a Secondary Node configured)
 - Master Node to eNodeB Change (X2 handover from an eNodeB with SN node to one

without a SN configured)

- eNodeB to Master Node

The Secondary Node configuration in the Handovers tab is only available if the Primary Node is set to an **eNodeB**.

List of known limitations:

- IRAT Handovers are not supported with to/from Master Nodes. If the test is configured to handover to/from a gNodeB towards a eNodeB with a gNodeB associated as a Secondary Node, it will throw an error at runtime.
- X2 Handover support between eNodeBs – only S1-MME signaling is supported (no 4G full core support).

Handover configuration parameters

The following table describes these objective parameters.

Parameter	Description
<i>Handover:</i>	
Only Once	<p>When this option is selected, the test performs a single iteration of the objective. Therefore, each UE moves through the entire mobility path, but only one time.</p> <p>When this option is not selected, the test executes handovers at the specified rate during the entire duration of the test. In this case, the UEs may move through the mobility path more than once.</p>
Rate	The rate at which handovers are initiated, measured in handovers per second.
Max Outstanding	The maximum number of Handover 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 between entering sustain time and the first handover.
Force N2 Handover	Select this check-box to force N2 handover with direct forwarding instead of 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	<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

Parameter	Description
Returning to Parent Node	<p>Handover to parent RAN, depending on what state the UE is before executing the procedure.</p> <ul style="list-style-type: none"> • 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.

Visited gNodeBs/eNodeBs : A list of the NG-RANs that UEs will visit during the test.

	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.
Secondary Node	This option is available only if the Primary Node is set to an eNodeB value. Select the secondary node from the drop-down list.

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>	
Only Once	When this option is selected, the procedure is ran only once for each subscriber. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.

Parameter	Description
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 time (in seconds) to wait before starting the secondary objective, after sustain is reached.
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.

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 the Enter/Exit Idle procedure is set and the UE has to exit Idle to perform a different procedure, the Enter/Exit Idle procedure is still scheduled to perform Exit Idle, but the UE is not in Idle anymore. In this case, 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>	
Only Once	When this option is selected, the test performs a single iteration of the objective. Therefore, each UE enters and exits the CM-IDLE state, but only one time. When this option is not selected, the test executes enters and exits the CM-IDLE state at the specified rate during the entire duration of the test. In this case, the UEs may enter and exit the CM-IDLE state more than once.
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.

Parameter	Description
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 that will elapse before the start of the Idle transition event simulation.
Interval	The number of seconds to wait between each successive state transition.

Create/Delete QoS Flows

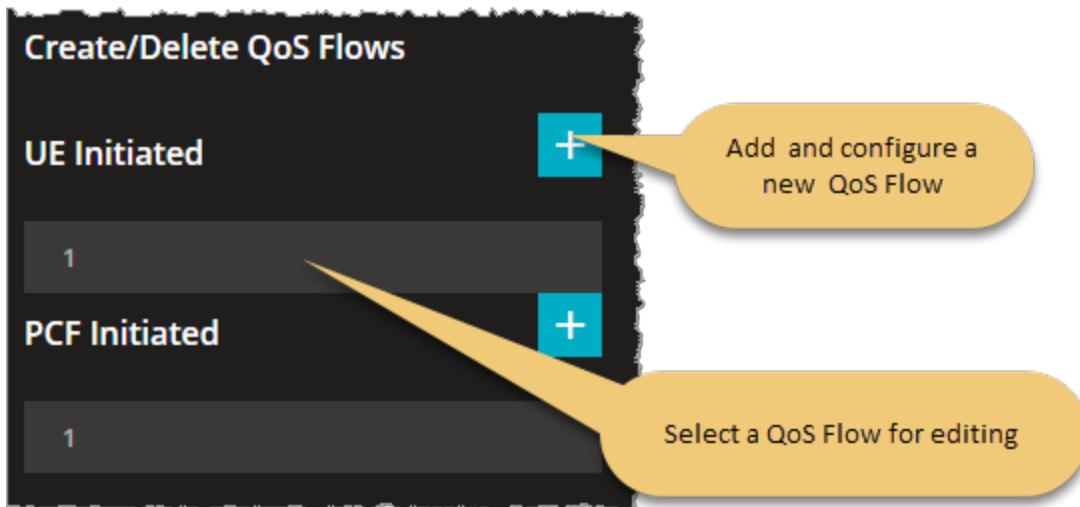
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured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



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.)

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.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameter requires a large number of UEs configured in the test in order to achieve the desired rate.
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.

Parameter	Description
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain timer.
Interval	Interval between the triggering of creation and deletion of the QoS flow, in seconds.
DNN	Select the DNN value for the drop-down list. For example: dnn.keysight.com.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

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.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameter requires a large number of UEs configured in the test in order to achieve the desired rate.
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 timer.
Interval	The interval between the triggering of creation and deletion of the PDU Session, in seconds.

Parameter	Description
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.

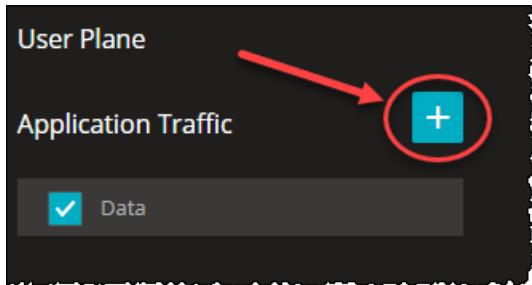
The following table describes the objective parameters.

Parameter	Description
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameter requires a large number of UEs configured in the test in order to achieve the desired rate.
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 timer.
Destination MSISDN	The destination MSISDN for the SMS text message.
Destination MSISDN Increment	The increment for the destination MSISDN.

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.

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



The available traffic applications are: **Stateless UDP**, **Data**, **Voice**, **Video OTT**, **DNS Client** and **Predefined Applications**.

NOTE

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

The following table describes the Application Traffic generation parameters.

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

Parameter	Description
	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 .

Stateless UDP Traffic

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

The following table describes the Stateless UDP parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Flow Type	This field is set to uplink and can not be modified since on the UE you can only configure the uplink flow.
Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The time to wait before the application traffic flows start.
Destination IP Address	The destination IP address to place in the IP packet.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .
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 on page 93 .
Fallback to	This option supports use cases in which it is desirable for user traffic to use the

Parameter	Description
Default Flow	<p>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>
Ethernet Device ID	Select the associated ethernet device that will be used to generate this flow.
Destination MAC Address	The destination MAC address to be used for sending this traffic flow as Ethernet traffic encapsulated in GTP. If left blank, ARP or ICMPv6 protocols will be used to learn the destination MAC address.

Data Traffic

The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Objective Type	By default, this parameter is set to Throughput 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.
Total Throughput (kbps)	The desired maximum throughput (in kbps) for the combined traffic flows that will be generated.
Application	Each Application Traffic entry requires at least one traffic flow definition, and can

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

Parameter	Description
Connection	
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Config on page 256).
QoS FlowID	Select a QoS Flow ID for this flow.

Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
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.
Call Type	Select the type of call from the drop-down list. Available options are: <ul style="list-style-type: none"> • Basic Call • Basic Call Mo (Mobile Originated) • Basic Call Mt (Mobile Terminated)
<i>Dial Plan:</i>	<i>For the settings required to configure the dial plan, refer to Dial Plan.</i>
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore 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

Parameter	Description
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
<i>Media settings:</i>	<i>For the configuration of media settings, refer to Media Settings.</i>

Dial Plan

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

Parameter	Description
Iterations	The number of times the Voice flow will be executed. It can be finite or infinite (set to zero).
DNN ID	Select the DNN from the drop-down list.
Source Phone	The URI assigned to the first simulated user, incremented by 1 for each UE.
Destination Phone	The URI assigned to the first simulated user, incremented by 1 for each UE.
Destination IP	The destination IP address.
Destination Port	The destination port number.

Media Settings

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

Parameter	Description
Audio Duration (ms)	Length of time to play the audio stream. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID	The QoS Flow ID for RTP traffic. Select the QoS Flows ID(s) 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>	

Parameter	Description
	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-WD

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.

Parameter	Description
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 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 .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.

Parameter	Description
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. 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.
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. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.
<i>Flow:</i>	
	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 APPLE 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.

Parameter	Description
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
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero).
Percentage	The percentage of total Objective Simulated Users 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(sec)	Set the number of seconds to wait before playback. The default value is 30.
Maximum Size(sec)	Set the number of seconds to be buffered on the client side. The defult value is 500.
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> • Adaptive Bitrate(ABR) • 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 Bitrate .
<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.

Parameter	Description
<i>Quality Shift</i>	
	Select this button to remove this play profile from your test configuration.
Shift Type	Select the shift type from the drop-down list. Available options <ul style="list-style-type: none"> • Stay at Current Bitrate • Change to the Lowest Bitrate • Change to the Lowest Bitrate • Change to the Lower Bitrate • Change to the Higher Bitrate
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to Change to Higher Bitrate or Change to Lower Bitrate .
Play Until End	If this check box is selected, the Play duration field is disabled and the original playtime is used.
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.

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.
Close TCP Connection After Each Transaction	Select the check box to terminate the TCP connection after each transaction.
Enable DNS Query Per Connection	Select the check box to process only one DNS query per TCP connection.

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
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none">• Simulated Users, or• Transactions Rate
Transactions rate	IMPORTANT This parameter is available only when Objective Type is set to Transactions Rate . Set the value for the transaction rate parameter.
Connection multiplier (per UE)	Set the value for the connection multiplier.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. 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.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Application Traffic Flows	Each Application Traffic entry requires at least one 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. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings. Refer to DNS Client Traffic on the previous page (below) for a description of the configuration settings for these traffic flows. Also, you can add custom parameters , based on your test configuration requirements.

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
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 on page 256).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

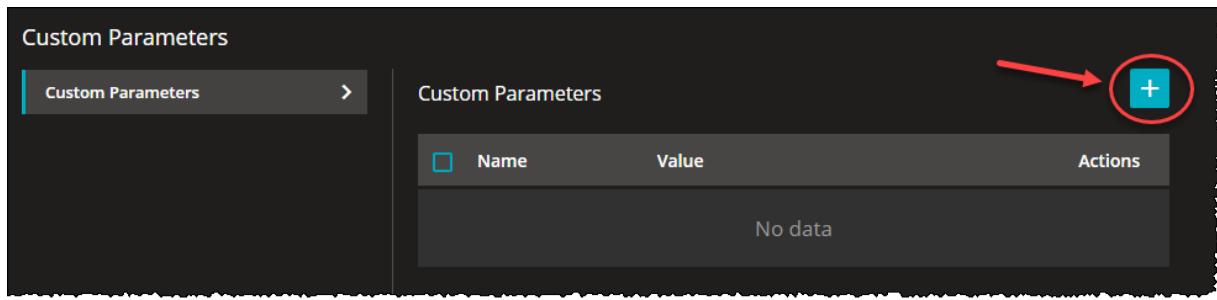
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

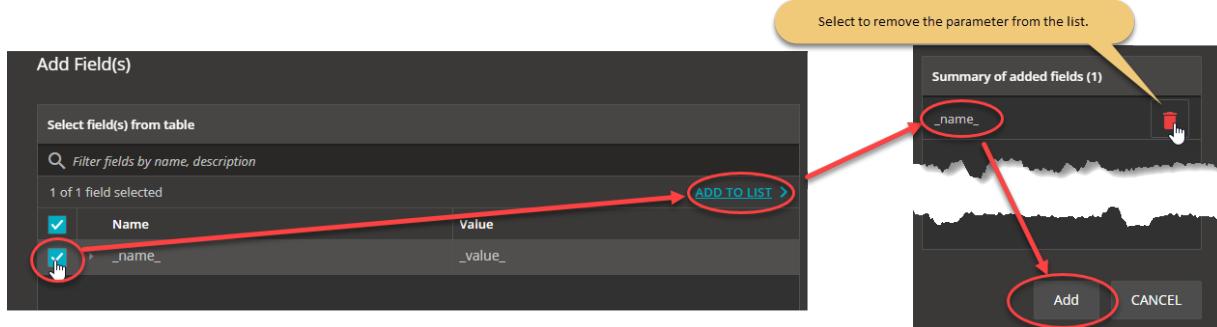
2. Select the **Add** button.



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 ...



Predefined Applications Traffic

The following table describes the Predefined Flows Traffic parameters.

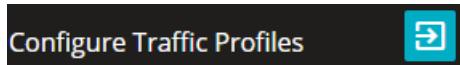
Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> Simulated Users Throughput Connections Per Second
Throughput (kbps)	IMPORTANT This parameter is available only when <u>Objective Type</u> is set to Throughput . The desired maximum throughput (in kbps) for the combined traffic flows that will be generated.
Connections Per Seconds	IMPORTANT This parameter is available only when <u>Objective Type</u> is set to Connections Per Second . Set the number of connections.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.

Parameter	Description
	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.
Configure Traffic Profiles	Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions. Refer to Traffic Profile on the facing page (below) for a description of the configuration settings for these traffic profiles.

Traffic Profile

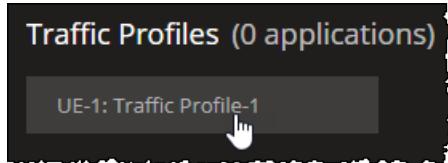
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

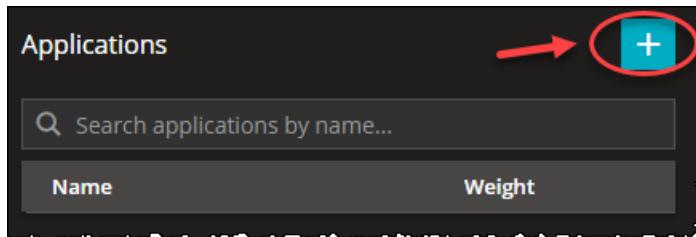
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

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.



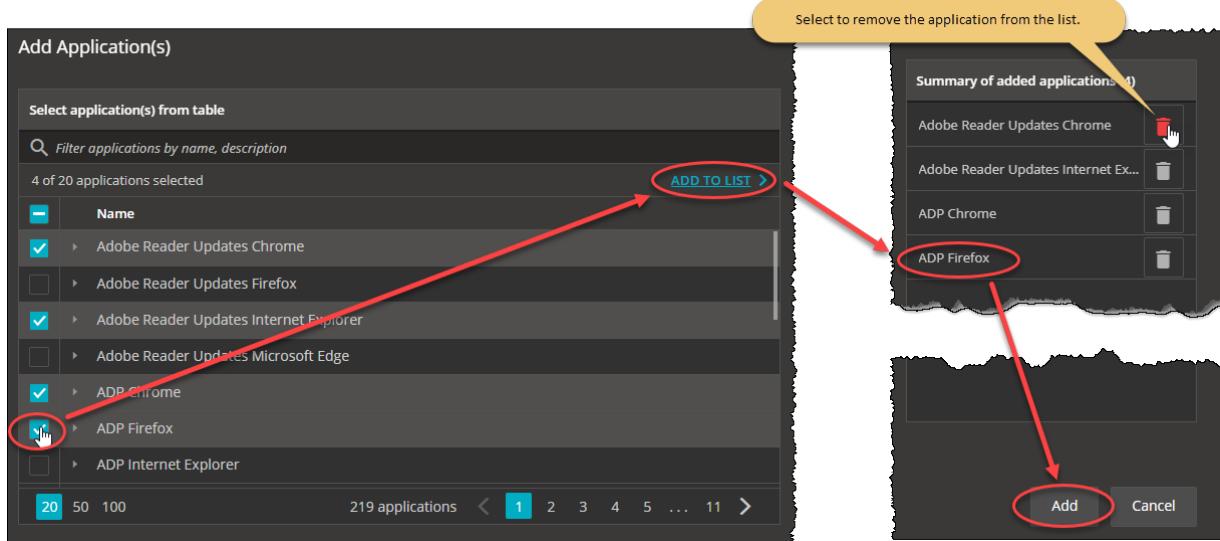
The Add Application(s) window opens.

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 ...

Applications		Edit	+
Search applications by name...			
Name	Weight		
Adobe Reader Updates Chrome 1	1		
Adobe Reader Updates Internet Exp...	1		
ADP Chrome 3	1		
ADP Firefox 4	1		

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

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

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

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

For example ...

The screenshot shows the 'Applications' configuration interface. On the left, there is a list of predefined applications with columns for 'Name' and 'Weight'. One application, 'Adobe Reader Updates Chrome 1', is selected and highlighted with a blue border. On the right, two sections are displayed: 'Application Settings' and 'Application Actions'.

Application Settings

- Destination Hostname: A text input field containing 'dnn.keysight.com'.
- DNN ID: A dropdown menu set to 'dnn.keysight.com'.
- QoS Flow ID: A dropdown menu set to '1'.

Application Actions

Actions

- A search bar labeled 'Search actions by name...'.
- A table listing actions:

#	Name
1.	Check For Updates Client -> Server acroipm2.adobe.com
2.	Download Updates Client -> Server ardownload.adobe.com

Application Settings

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

NOTE

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

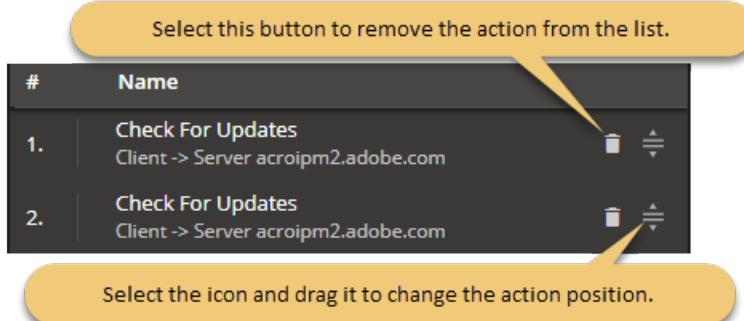
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

Application Actions

The Application Actions section lists the actions and action parameters available in LoadCore 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:

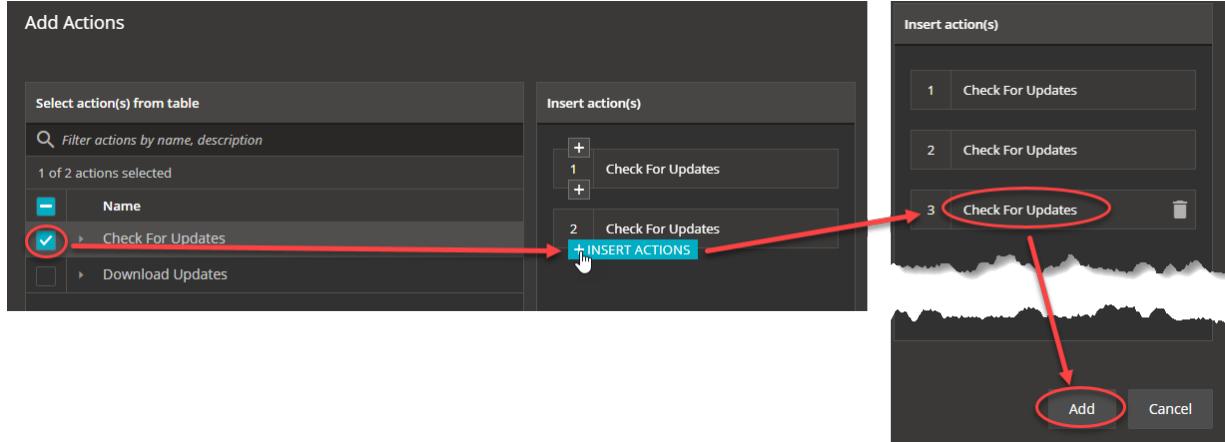
1. Use the icons available for each icon in order to remove it or to change its position in actions list.
For example ...



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 ...



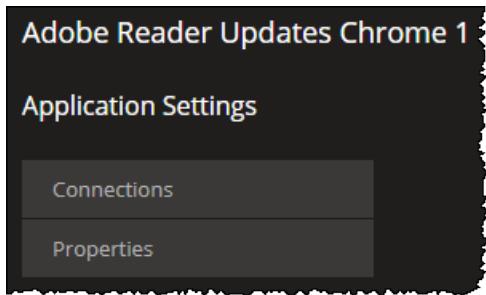
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

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.

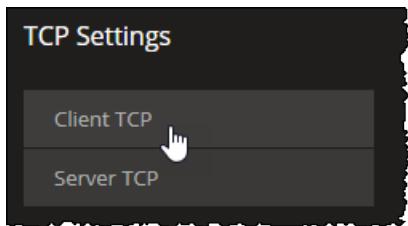
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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

TCP Settings

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



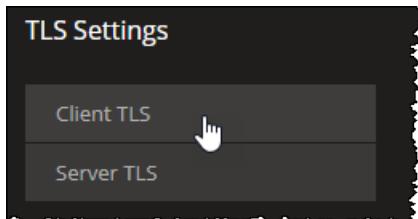
These parameters are configurable for both Client and Server settings, as presented in the following table.

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

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

TLS Settings

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



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
TLSv1.2	Select the check box to enable it. The following options became available:

Parameter	Description
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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> NOTE Session reuse method is available only if TLSv1.2 is selected. </div>
Immediate close	Select the check box to enable it.
TLSv1.3	<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 compatibility	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	Select the check box to enable it.

Server TLS Settings

Parameter	Description
TLSv1.2	<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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> NOTE Session reuse method is available only if TLSv1.2 is selected. </div>
Immediate close	Select the check box to enable it.
TLSv1.3	<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	Select the check box to enable it. It allows for compatibility with middleboxes

Parameter	Description
compatibilty	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>
<i>Key file password</i>	<i>Enter your key file password.</i>
<i>DH file Traffic</i>	<i>Select Upload to add your DH file or Clear to remove it.</i>

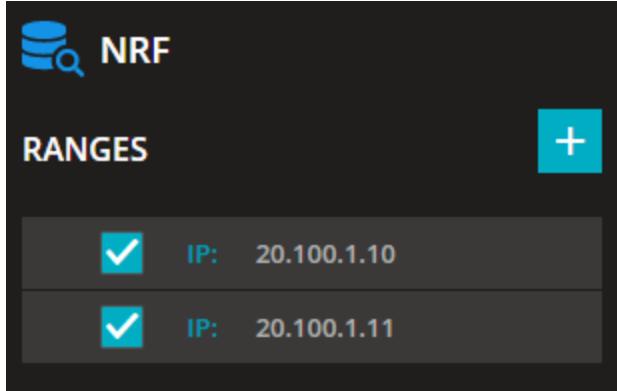
NF Discovery service

The NF Repository Function (NRF) enables a service discovery function (Nnrf_NFDiscovery service) that allows a Network Function instance to discover services offered by other Network Function instances, by querying the local NRF. For a 5G node to be discovered, it must be registered to an NRF.

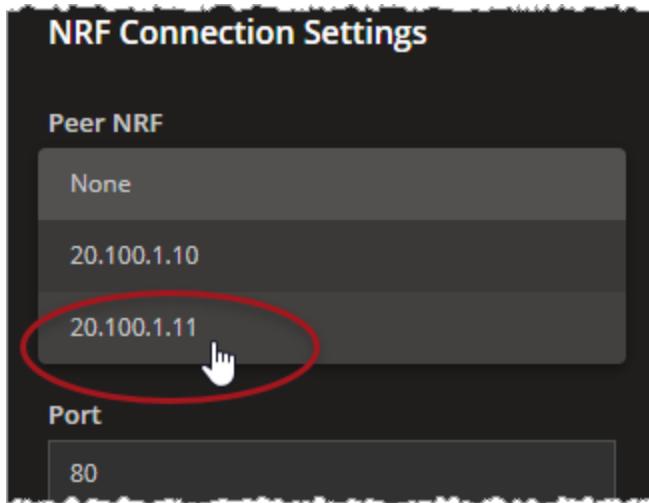
NF Discovery in LoadCore

To use NF Discovery in a LoadCore test:

1. Enable and configure one or more NRF nodes for the test. For example:



2. To register a node (such as an SMF) for discovery:
 - a. Select that node from the topology window, then select the range that you are registering.
 - b. From **Range Settings**, select **Remote SBA Nodes**.
 - c. Select **NRF Connection Settings**, and then select the desired *Peer NRF* (the IP address of the peer NRF). For example:

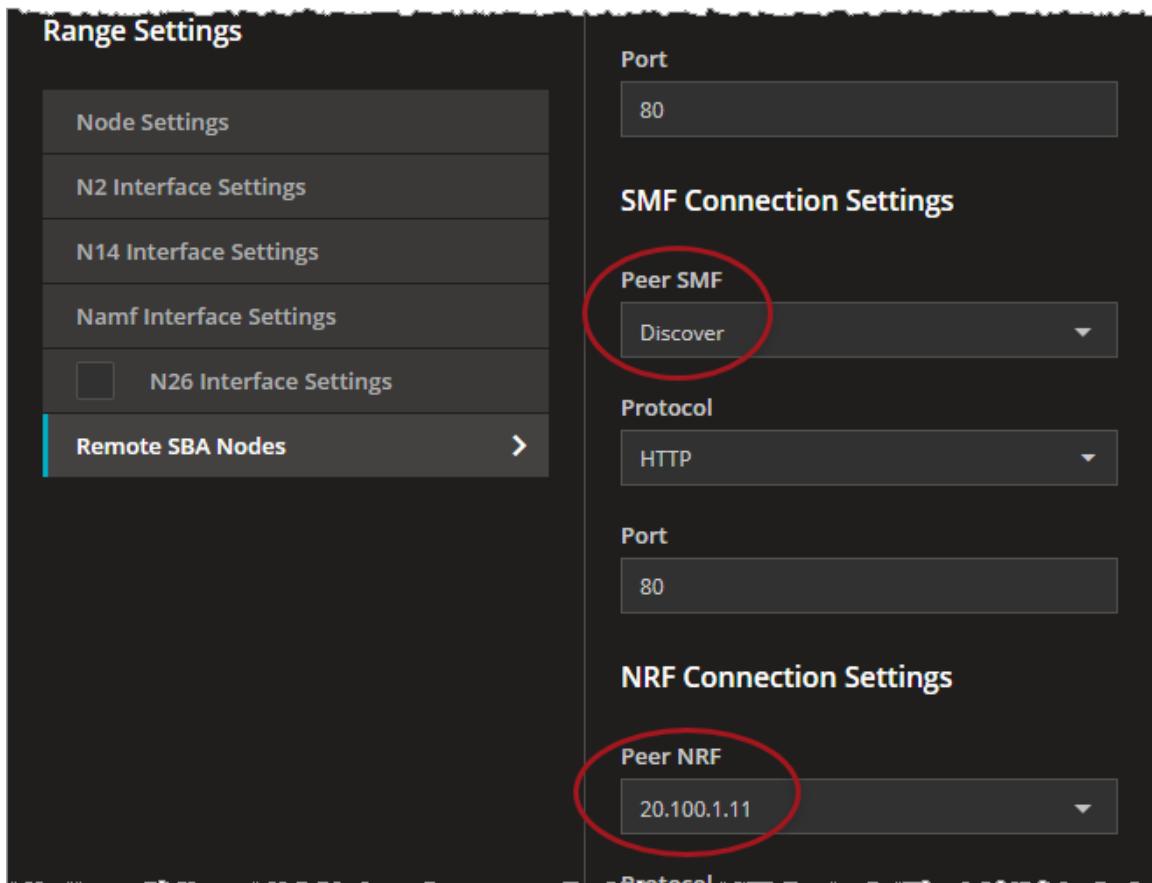


This is the NRF to which the node is registering.

3. For a node (such as an AMF) that needs to discover services offered by another NF instance:

- a. Select that node from the topology window, then select the range that will query the NRF.
- b. From the **Remote SBA Nodes** panel, select **Discover** in the *Peer NRF* field for the node to be discovered.
- c. Also from the **Remote SBA Nodes** panel, select **NRF Connection Settings**, and then select the desired *Peer NRF* (the IP address of the NRF to which the node is registered).

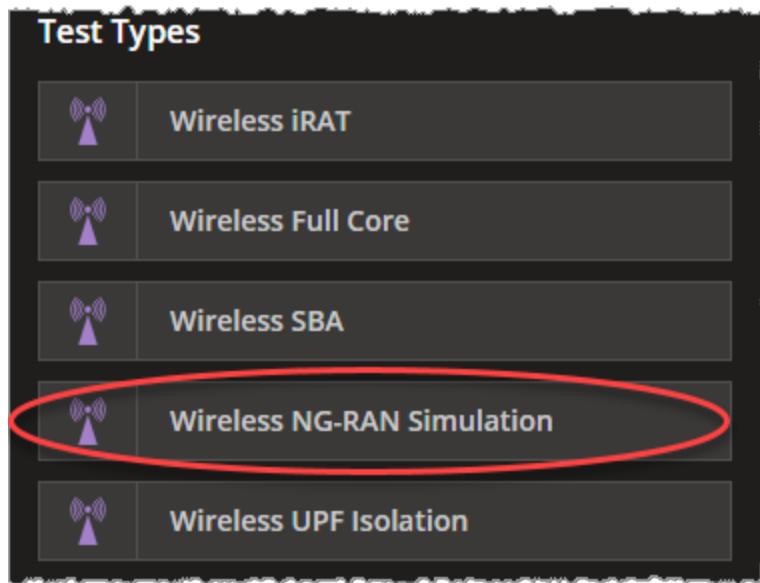
For example:



CHAPTER 7

NG-RAN Simulation tests

To create an **NG-RAN simulation test**, select this test type from the list of available Test Types:



The NG-RAN simulation test topology is similar to a Full Core test, except that:

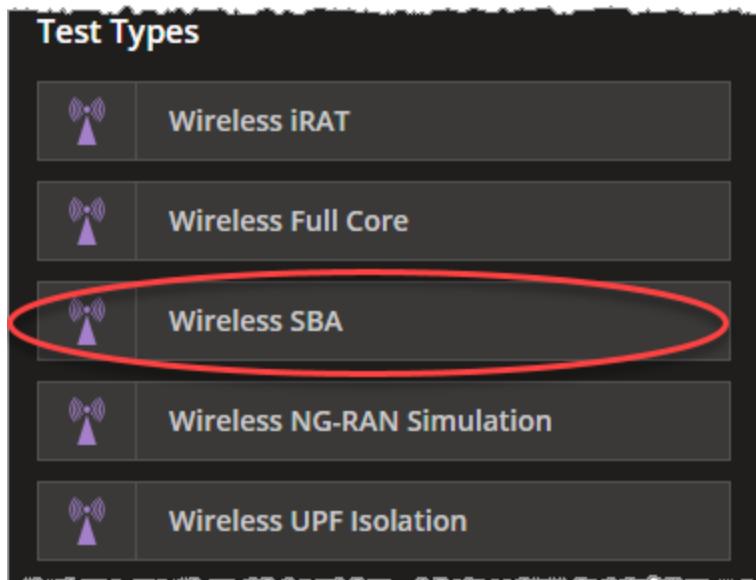
- The AMF and UPF nodes are configured as DUTs.
- The UE, RAN, and DN nodes are enabled for testing.
- All other simulated nodes are disabled by default.

For more details about configuring a Full Core test, refer to [Full Core tests: configuration settings](#).

CHAPTER 8

SBA tests: configuration settings

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

**Topics:**

SBA Tester overview	311
SBA Tester Global Settings panel	312
Connection Settings	314
Advanced Settings	314
Impairment	316
DNNs panel	317
DNN configuration settings	318
DNN GBR configuration settings	320
Session AMBR configuration settings	320
QoS Flows panel	321
QoS Flow configuration settings	322

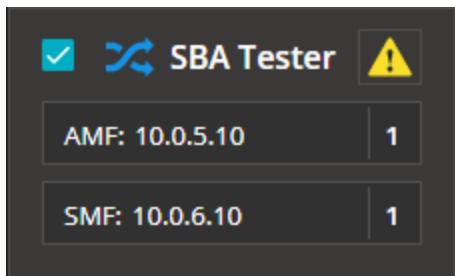
QoS Flow Packet Filter configuration settings	324
QoS Flow Maximum Packet Loss configuration settings	325
QoS Flow ARP configuration settings	325
QoS Flow MBR configuration settings	326
QoS Flow GBR configuration settings	326
SBA Tester Simulated Nodes panel	327
AMF configuration settings	327
SMF configuration settings	330
PCF configuration settings	333
SBA Tester Remote SBA Nodes	335
SBA Tester Remote Nodes	336
NRF configuration settings	337
NRF Ranges panel	338
NRF Range panel	338
NRF node settings	339
NRF Nnrf interface settings	340
SCP configuration settings	341
SCP Ranges panel	341
SCP Range panel	342
SCP interface settings	343
SCP Remote SBA Nodes	343
AUSF configuration settings	345
AUSF Ranges panel	346
AUSF Range panel	346
AUSF node settings	347
AUSF Nausf interface settings	348
AUSF remote SBA nodes	349
PCF configuration settings	351
PCF Ranges panel	351
PCF Range panel	352
PCF node settings	353
PCF service area restrictions	353

PCF Npcf interface settings	355
PCF remote SBA nodes	356
UDR configuration settings	356
UDR Ranges panel	356
UDR Range panel	357
UDR Nudr interface settings	358
UDR remote SBA nodes	359
UDM configuration settings	359
UDM Ranges panel	359
UDM Range panel	360
UDM node settings	361
UDM Nudm interface settings	364
UDM remote SBA nodes	365
CHF configuration settings	365
CHF Ranges panel	366
CHF Range panel	366
CHF node settings	367
CHF Nchf interface settings	367
CHF remote SBA nodes	368
NSSF configuration settings	370
NSSF Ranges panel	371
NSSF Range panel	371
NSSF node settings	372
Nnssf Interface Settings	373
Remote SBA nodes	374
NSSF Restricted NSSAIs	375
NSSF Network Slices	376
NSSF Configured NSSAI	377
UE configuration settings	378
UE Ranges panel	379
UE Range panel	379
Range Settings	380

UE Identification	381
UE Security	381
UE Settings	383
UE SDF settings	384
Shared Data IDs	385
UE Subscribed AMBR settings	385
Service Area Restrictions	385
Forbidden Areas	386
Notifications	387
Network Slicing	388
UDM Default NSSAI settings	389
UDM SNSSAI Mappings	389
UDR SNSSAI Settings	390
Charging Function	390
Policy Counters	391
Notify Policy Counters	392
Objectives	394
Primary Objective	395
About primary objectives	396
Active subscribers	398
Subscribers per Second	403
Secondary Objectives	408
UEGetNSSAIAMF2UDM	409
RegistrationAMF2UDM	410
DeregistrationAMF2UDM	411
GetPolicyAMF2PCF	412
UpdatePolicyAMF2PCF	413
GetPolicySMF2PCF	415
UpdatePolicySMF2PCF	416
RegistrationSMF2UDM	418
DeregistrationSMF2UDM	419
IntermediateSpendingLimitPCF2CHF	419

SBA Tester overview

The purpose of the **SBA test** test type is to test one of the SBA nodes by configuring what procedures you want to simulate and with what rate. This way, you can replace some nodes of the network architecture with a single **SBA Tester** node.



This SBA Tester hides the rest of the nodes and acts as if those nodes initiated certain procedures. The main advantage of this approach is that by doing this you can isolate one or a few interfaces and get rid of the overhead of simulating the rest of the needed interfaces between nodes, and thus obtaining a higher performance and greater flexibility.

In contrast, in the Full Core test topology, you do not actually control the rate at which the messages reach AUSF; rather, you control the rate at which you want the UE to do certain actions, and the rate at which messages reach AUSF is, consequently, determined by what happens in the network.

For example ...

You can test an AUSF node with the Full Core topology test. To do this, you can configure a UE and make it attach to the network. When that UE attaches, the network needs to establish sessions for it on the AMF, the SMF, the UPF, and the NG-RAN, and at some point a request reaches AUSF.

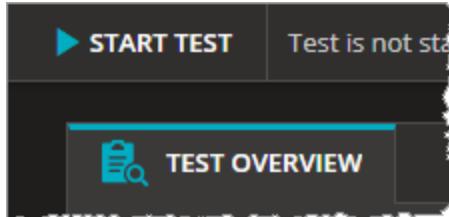
Now if you use the SBA Tester to test the AUSF, you can just select the procedure you want to reach the AUSF, and with what rate. The messages associated to the selected procedure will be sent directly to the AUSF. From the AUSF's point of view, given the fact that the message structure and sequence is correct, it can only assume that these messages are generated by the same procedure as in the Full Core topology and it has no way of telling that those nodes are not actually there.

SBA Tester Global Settings panel

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:

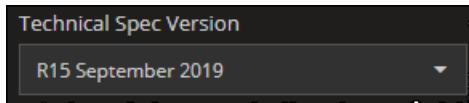


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



LoadCore 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:

Connection Settings	314
Advanced Settings	314
Impairment	316
DNNs panel	317
DNN configuration settings	318
DNN GBR configuration settings	320
Session AMBR configuration settings	320
QoS Flows panel	321
QoS Flow configuration settings	322
QoS Flow Packet Filter configuration settings	324
QoS Flow Maximum Packet Loss configuration settings	325
QoS Flow ARP configuration settings	325
QoS Flow MBR configuration settings	326

QoS Flow GBR configuration settings	326
---	-----

Connection Settings

The following table describes the general connection settings that you configure for the SBA Tester.

Setting	Description
Connection Start Rate	The rate for TCP connection establishment.
Connection Stop Rate	The rate for TCP connection termination.
Max Requests Per Connection	The maximum requests count that should be sent over a TCP connection before it is closed.

Advanced Settings

The following table describes the settings required to enable control plane advanced statistics and packet capture on the assigned agents.

Setting	Description
Overwrite Capture Size for IxStack	Select this check box 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 check box to enable it.
Enable Capture On Loopback Interface	Select this check box to enable packet capture on the loopback interface.
Enable Control Plane Advanced Stats	By default, these measurements and statistics are disabled. Select this option to enable control plane latency statistics.
Automated Polling Interval	Selected by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval	This option becomes available only when Automated Polling Interval check box is unselected. It allows you to create a custom polling interval.

Setting	Description
(sec)	
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.
Ignore Offline Agents At Runtime	When this option is selected, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.

Control Plane Latency Statistics

For the Control Plane Latency Statistics, the latency is measured per HTTP transaction.

For the control plane HTTP latency statistics, on the client side, the latency measures the time between the moment when the request is sent and the moment when the answer is received. On the server side, the latency measures the time between the moment when the request is received and the moment when the answer is sent.

IMPORTANT

The time shown in statistics may be slightly different than the time computed in any capturing tool (for example, Wireshark) because of the time when the packets are actually captured.

Latency buckets:

- 0us - 125us
- 125us - 250us
- 250us - 500us
- 500us - 1ms
- 1ms - 5ms
- 5ms - 10ms
- 10ms - 15ms
- 15ms - 20ms
- 20ms - inf

NOTE

If enabled, the control plane latency statistics will not be displayed in predefined dashboards in LoadCore statistics user interface. To display these statistics you will need to use custom dashboards.

Retrieve captured packets

After enabling packet capture, and running the test, to download the generated packet captures, you need to use a SFTP client (for example, WinSCP) to retrieve the captures from `/opt/5gc-test-engine` on each of the agents.

The packet capture can be identified as follows:

- `latestCapture.pcap`, when running the test without DPDK activated.
- `latestIxStackCapture.pcap` when running the test with DPDK activated.

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 LoadCore or overwrite it with your own value.
Action Type	Select an option from the drop-down list: <ul style="list-style-type: none"> Custom script PFCP-drop message
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.

DNNs panel

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

When setting up a LoadCore test, these DNN configurations become immediately available for selection in the UDM and UE configurations.

Accessing the configuration settings

To access the DNN configuration settings, select **DNNs** from the **Global Settings** panel. LoadCore 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	318
DNN GBR configuration settings	320
Session AMBR configuration settings	320

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
	Select the Delete DNN button to delete this DNN from your test configuration.
DNN	<p>Enter the DNN value for this DNN definition. For example: <code>dnn.keysight.com</code>.</p> <p>A DNN (as is the case with an EPS APN) is composed of two parts:</p> <ul style="list-style-type: none"> • A mandatory Network Identifier that defines the external network to which the UPF is connected. • 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>
Address	The IP address of the DNN.
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	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

Setting	Description
	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.
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	The IPv4 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv4 addresses.
IPv6 Index	The IPv6 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv6 addresses.
EPS Interworking	Select this option if the UE subscription data indicates support for interworking with EPS for this DNN.
Is Local Area DN	<p>Select this option if connectivity with the DNN is provided through a Local Area Data Network (LADN).</p> <p>A Local Area Data Network is a DN that is accessible by the UE only in specific locations, that provides connectivity to a specific DNN, and whose availability is provided to the UE.</p>
ADC Support	Select this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.
Subscriber Spending Limits	Select this option if the DNN will support PDU session policies that are based on subscriber spending limits.
Offline	Select this option if the DNN will support the offline charging method for PDUs sessions.
Online	Select this option if the DNN will support the online charging method for PDUs sessions.
GBR	Select this option to open a new panel that contains the GBR settings. These settings are described in DNN GBR configuration settings on the next page .
Session AMBR	Select this option to open a new panel that contains the Session AMBR settings. These settings are described in Session AMBR configuration settings on the next page .

DNN 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 **GBR** settings are described in the table that follows.

Setting	Description
Guaranteed Bit Rate Uplink	The guaranteed bit rate (bps) for uplink traffic. This is the uplink bit rate that the QoS Flow associated with this DNN is expected to provide.
Guaranteed Bit Rate Downlink	The guaranteed bit rate (bps) for downlink traffic. This is the downlink bit rate that the QoS Flow associated with this DNN is expected to provide.

Session AMBR configuration settings

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

- The main DNN settings, described in [DNNs panel on page 317](#).
- The DNN's Session AMBR settings, described below.

The following tables describes the Session AMBR configuration settings.

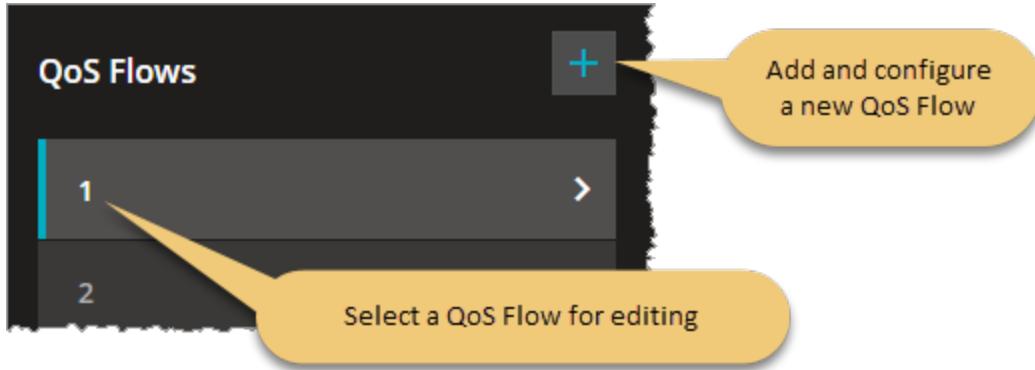
Parameter	Description
Session AMBR Uplink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Session AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Session AMBR Downlink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) downlink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

QoS Flows panel

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

Accessing the configuration settings:

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



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

QoS Flow configuration settings	322
QoS Flow Packet Filter configuration settings	324
QoS Flow Maximum Packet Loss configuration settings	325
QoS Flow ARP configuration settings	325
QoS Flow MBR configuration settings	326
QoS Flow GBR configuration settings	326

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.

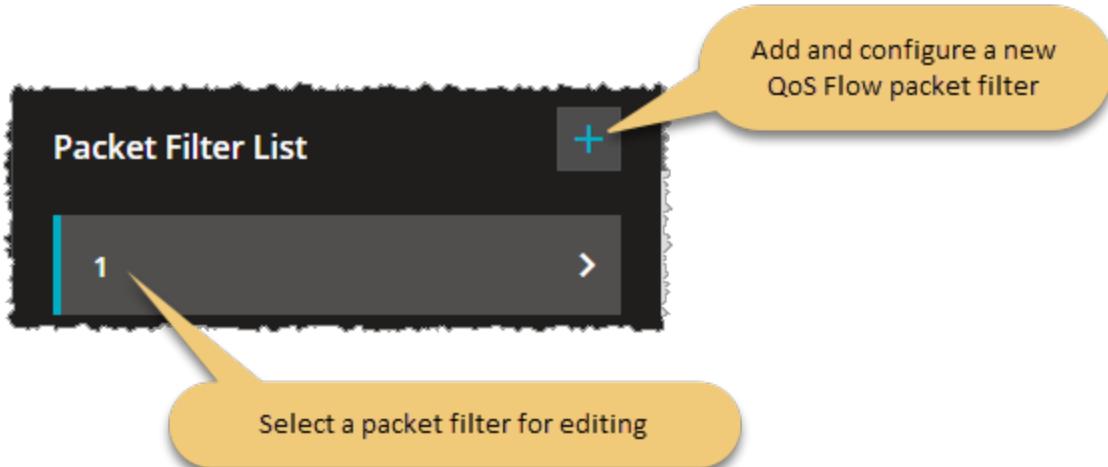
Setting	Description
<i>QoS Flow:</i>	
Is Default	Select this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow. If this option is not selected, LoadCore makes the Packet Filter List settings available for configuration (refer to QoS Flow Packet Filter configuration settings on page 324 for descriptions of these settings).
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	Specify the 5QI value (decimal number). 5G QoS Identifier (5QI) is a scalar that is used as a reference to 5G QoS characteristics defined in TS 23.501, clause 5.7.4. These are access node-specific parameters that control QoS forwarding treatment for the QoS Flow (such as scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, among others). Standardized 5QI values have a one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in TS 23.501, table 5.7.4-1.
5QI Priority Level	Specify the 5QI Priority Level for this QoS Profile. 5QI Priority Level is a Policy Control parameter that accepts values from 1 through 127 (where 1 is the highest priority). It indicates a priority in scheduling resources among QoS Flows.
Resource Type	Select the type of resource that the QoS Flow requires: Guaranteed Bit Rate (GBR), Non-Guaranteed Bit Rate, or Delay Critical GBR. The Resource Type determines whether 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 5GI. Each GBR QoS Flow is associated with an <i>Averaging window</i> . It represents the time duration (specified in milliseconds) over which the GFBR and MFBR are calculated.

Setting	Description
QoS Rule Precedence	<p>Specify the desired QoS Rule Precedence value for this QFI.</p> <p>The QoS rule precedence value (and the PDR precedence value) determine the order in which a QoS rule or a PDR, respectively, will be evaluated. The evaluation of the QoS rules or PDRs is performed in increasing order of their precedence value.</p>
Packet Delay Budget	<p>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.</p>
Packet Error Rate	<p>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.</p>
Max Data Burst	<p>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.</p>
Notification Control	<p>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.</p>
Segregation	<p>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.</p>
Packet Filter List	<p>IMPORTANT This is available if Is Default option is not selected.</p> <p>Refer to the following topic for a description of the Packet Filter configuration settings: QoS Flow Packet Filter configuration settings on the next page.</p>
Max Packet Loss Rate	<p>Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: QoS Flow Maximum Packet Loss configuration settings on page 325.</p>
ARP	<p>Refer to the following topic for a description of the ARP configuration settings: QoS Flow ARP configuration settings on page 325.</p>
MBR	<p>Refer to the following topic for a description of the MBR configuration settings: QoS Flow MBR configuration settings on page 326.</p>
GBR	<p>Refer to the following topic for a description of the GBR configuration settings: QoS Flow GBR configuration settings on page 326.</p>

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.

Setting	Description
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 Maximum Packet Loss configuration 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	<p>Specify the ARP priority level.</p> <p>The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the</p>

Setting	Description
	home network and thus applicable when a UE is roaming.
Preemption Capability	Select this option if the packets in this QoS Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.
Preemption Vulnerability	Select this option if the packets in this QoS Flow are candidates for being preempted by other flows. When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.

QoS Flow MBR configuration settings

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

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

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

QoS Flow GBR configuration settings

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

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

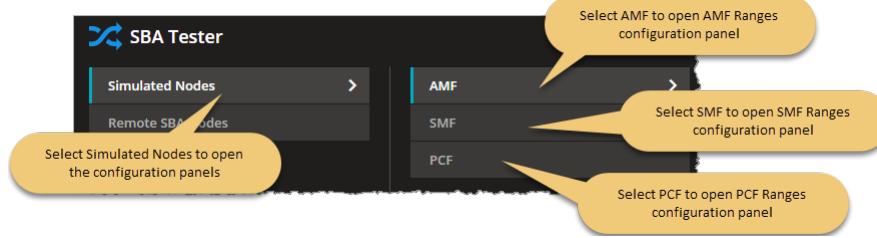
Setting	Description
<i>5G QoS Flow, GBR:</i>	
Uplink Bitrate Unit	Select the uplink bitrate unit from the drop-down list.
Uplink Bitrate Value	Set the guaranteed bit rate value for uplink traffic.
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set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

SBA Tester Simulated Nodes panel

The **Simulated nodes** panel opens when you select the SBA Tester from the network topology window. You can perform the following tasks from this panel:

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

When you select the Simulated Nodes panel, you enter the AMF/SMF/PCF test configuration Settings. Each range can be accessed and configured by selecting it.



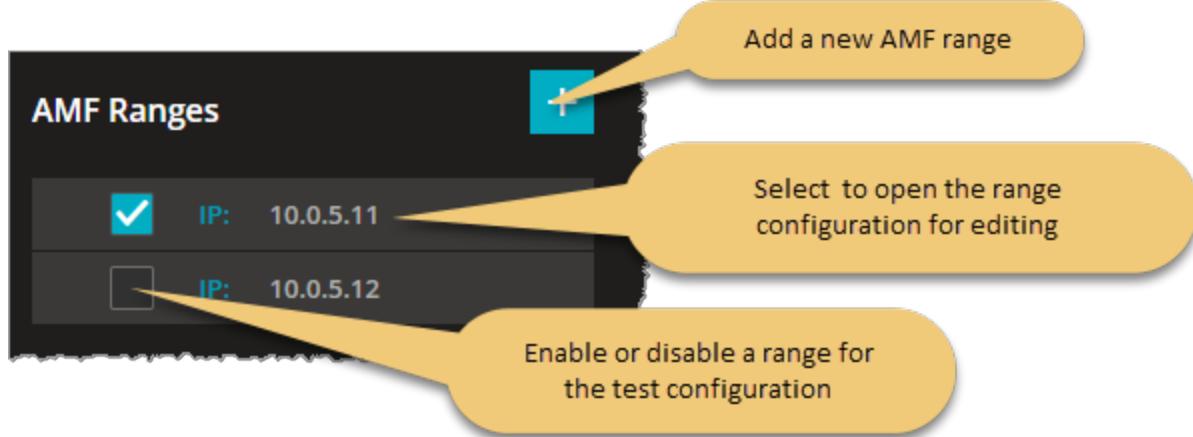
AMF configuration settings

The **AMF Ranges** panel opens when you select the AMF node from the Simulated Nodes panel.

You can perform the following tasks from this 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 can add and delete AMF ranges as necessary to support your test objectives.

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

Setting	Description
<i>AMF:</i>	
	Select the Delete Range button to delete this range from your test configuration.
<i>Namf Interface Settings:</i>	
Connectivity Settings	Each AMF range requires the configuration of Namf interface settings. These settings are described below in the AMF Namf interface settings on the facing page section.
<i>Node Settings:</i>	
Name	The name uniquely identifies each AMF instance. You can accept the value provided by LoadCore or overwrite it with your own value.
Instance ID	Each AMF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
MCC	<p>The PLMN MCC for this AMF range.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
MNC	<p>The PLMN MNC for this AMF range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Home Network Private Key	The home network private key.
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</p>

Setting	Description
	addresses the case that there are more AMFs in the network than the number of AMFs that can be supported by AMF Set ID and AMF Pointer. It allows operators to re-use the same AMF Set IDs and AMF Pointers in different regions.
Set ID	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). The AMF Set ID to use for this simulated AMF node. The Set ID uniquely identifies the AMF Set within the AMF Region.
Pointer	The AMF Pointer identifies one or more AMFs within the AMF Set.
Implicit Subscription Expiration from UDM	Select the check box inn order to enable it.
Subscription Duration (2)	Set the value for the subscription duration.
Use SCP Node	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes	This option is available only if the visible if Use SCP Node above check box is selected. It allows the user to select the target nodes (UDM, AUSF, PCF) for Indirect Communication via SCP.

AMF Namf interface settings

Namf is the service-based interface through which a AMF instance makes its services available to other services in a 5G network.

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

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

Connectivity Settings	Description
Increment	Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
TCP Connections	The number of concurrent TCP connections to use for each DUT.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

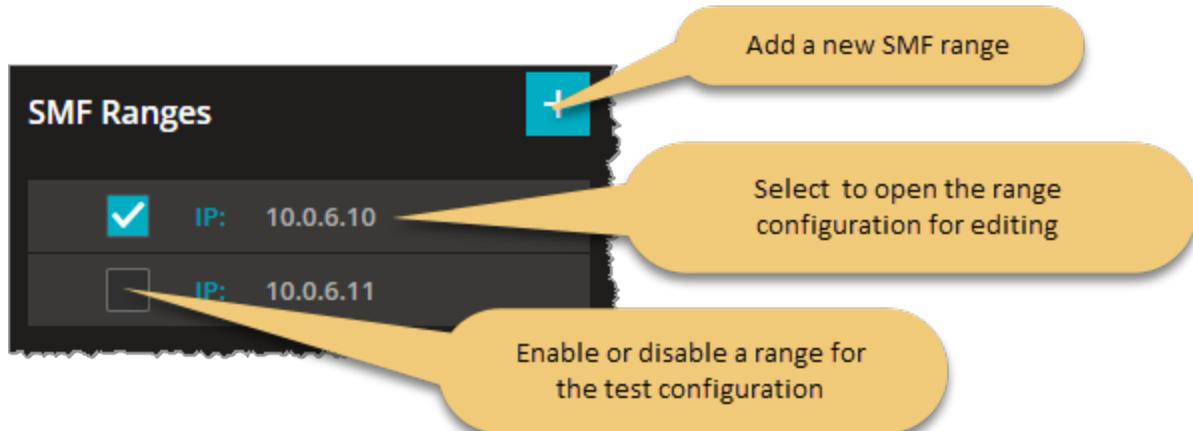
SMF configuration settings

The **SMF Ranges** panel opens when you select the SMF node from the Simulated Nodes panel.

You can perform the following tasks from this panel:

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

For example ...



You can add and delete SMF ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you need to configure for each SMF range.

Setting	Description
<i>SMF:</i>	
	Select the Delete Range button to delete this range from your test configuration.
<i>Nsmf Interface Settings:</i>	
Connectivity Settings	Each SMF range requires the configuration of Nsmf interface settings. These settings are described below in the SMF Nsmf interface settings on the next page section.
<i>Node Settings:</i>	
Instance ID	Each SMF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
PLMN MCC	<p>The PLMN MCC for this AMF range.</p> <p>About PLMN MCC ...</p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this AMF range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Use SCP Node	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes	This option is available only if the visible if Use SCP Node above check box is selected. It allows the user to select the target nodes (PCF) for Indirect Communication via SCP.
<i>SMF NSSAI:</i>	
	Select the Add NSSAI button to add a NSSAI to your test configuration.
<i>SMF NSSAI:</i>	

Setting	Description
	Select the Delete NSSAI button to remove this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
DNNs	A DNN (Data Network Name) with which PDU sessions will be associated for this NSSAI. Select one or more DNNs from the drop-down list.

SMF Nsmf interface settings

Nsmf is the service-based interface through which a SMF instance makes its services available to other services in a 5G network.

The following **Connectivity Settings** enable the necessary Nsmf 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 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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
TCP Connections	The number of concurrent TCP connections to use for each DUT.
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.
Inner VLAN	IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i>

Connectivity Settings	Description
	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.

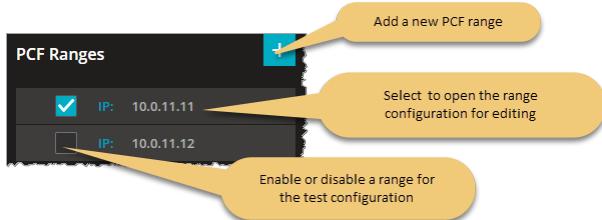
PCF configuration settings

The **PCF Ranges** panel opens when you select the PCF node from the Simulated Nodes panel.

You can perform the following tasks from this panel:

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

For example ...



You can add and delete PCF ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you need to configure for each PCF range.

Setting	Description
<i>PCF:</i>	
	Select the Delete Range button to delete this range from your test configuration.
<i>Npcf Interface Settings:</i>	
Connectivity Settings	Each PCF range requires the configuration of Npcf interface settings. These settings are described below in the PCF Npcf interface settings on the next page section.
<i>Node Settings:</i>	
Instance ID	Each AMF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
PLMN MCC	The PLMN MCC for this AMF range. About PLMN MCC ...

Setting	Description
	<p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this AMF range.</p> <p>About PLMN MNC ...</p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Use SCP Node	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes	This option is available only if the visible if Use SCP Node above check box is selected. It allows the user to select the target nodes (CHF) for Indirect Communication via SCP.

PCF Npcf interface settings

Npcf is the service-based interface through which a PCF instance makes its services available to other services in a 5G network. The following **Connectivity Settings** enable the necessary Npcf connectivity and service interaction.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
TCP Connections	The number of concurrent TCP connections to use for each DUT.
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.
Inner VLAN	<p>IMPORTANT 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.

SBA Tester Remote SBA Nodes

The **Remote SBA Nodes** panel opens when you select the SBA Tester from the network topology window.



NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

Setting	Description
Peer SCP	Select the IP address of the SCP node used as next hop.
Protocol	The protocol to use for communications. It can be either HTTP or HTTPS.
Port	The port number to use for communications. The default is port 80, but you can choose a different port number.

SBA Tester Remote Nodes

This section describes the configuration of the SBA Tester remote nodes.

NRF configuration settings	337
NRF Ranges panel	338
NRF Range panel	338
NRF node settings	339
NRF Nnrf interface settings	340
SCP configuration settings	341
SCP Ranges panel	341
SCP Range panel	342
SCP interface settings	343
SCP Remote SBA Nodes	343
AUSF configuration settings	345
AUSF Ranges panel	346
AUSF Range panel	346
AUSF node settings	347
AUSF Nauf interface settings	348
AUSF remote SBA nodes	349
PCF configuration settings	351
PCF Ranges panel	351
PCF Range panel	352
PCF node settings	353
PCF service area restrictions	353
PCF Npcf interface settings	355
PCF remote SBA nodes	356

UDR configuration settings	356
UDR Ranges panel	356
UDR Range panel	357
UDR Nudr interface settings	358
UDR remote SBA nodes	359
UDM configuration settings	359
UDM Ranges panel	359
UDM Range panel	360
UDM node settings	361
UDM Nudm interface settings	364
UDM remote SBA nodes	365
CHF configuration settings	365
CHF Ranges panel	366
CHF Range panel	366
CHF node settings	367
CHF Nchf interface settings	367
CHF remote SBA nodes	368
NSSF configuration settings	370
NSSF Ranges panel	371
NSSF Range panel	371
NSSF node settings	372
Nnssf Interface Settings	373
Remote SBA nodes	374
NSSF Restricted NSSAIs	375
NSSF Network Slices	376
NSSF Configured NSSAI	377

NRF configuration settings



Network Repository Function (NRF) is the 5G core network service that allows every network function to discover the services offered by other network functions. It supports the service discovery function by maintaining the set of NF profiles and the set of available NF instances. It makes its services available to other network

functions through the Nnrf service-based interface. Multiple instances of NRF may be deployed, with each instance storing specific data.

Topics:

NRF Ranges panel	338
NRF Range panel	338
NRF node settings	339
NRF Nnrf interface settings	340

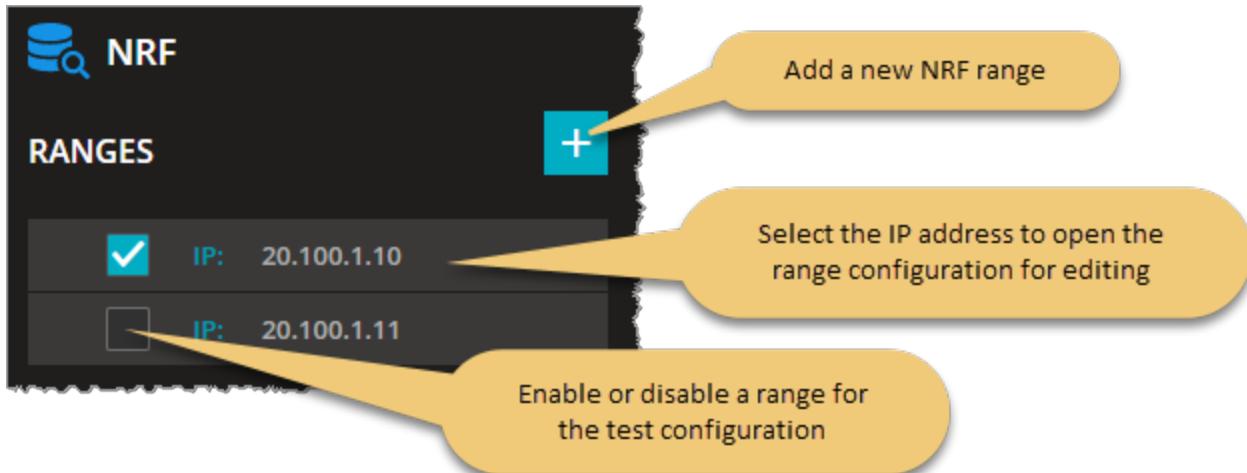
NRF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...

**NRF Range panel**

You add and select NRF ranges from the NRF Ranges panel. When you select the IP address of a NRF , LoadCore opens the **Range** panel, from which you can:

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

NRF range controls and settings

Each NRF range is identified by a unique IP address. You can add and delete NRF ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each NRF 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 NRF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the NRF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each NRF range includes the configuration of an associated set of Node Settings, which are described in NRF node settings below .
Nnrf Interface Settings	Each NRF range requires the configuration of Nnrf interface settings, through which a NRF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in NRF Nnrf interface settings on the next page .

NRF node settings

Each NRF range includes a set of Node Settings.

Node Settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple NRF instances may be deployed in the 5G network. Each NRF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
MCC	Set the mobile country code. 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.
MNC	Set the mobile network code. About PLMN MNC ...

Setting	Description
	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.
Heartbeat Interval(s)	Time in seconds expected between 2 consecutive heartbeat messages from an NF Instance to the NRF.

NRF Nnrf interface settings

Nnrf is the service-based interface through which a NRF instance makes its services available to other services in a 5G network.

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

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT 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>

Connectivity Settings	Description
VLAN ID	VLAN identifier.

SCP configuration settings



Service Communication Proxy (SCP) allows the user to use Indirect Communication between SBA nodes. As of now, only model C is supported which uses the `3gpp-Sbi-Target-apiRoot` custom header. Spec version R16 September 2020 is required to use this feature.

The Service Communication Proxy (SCP) enables an important role within the 5G Service Based Architecture (SBA), providing functions ranging from simplifying network topology by applying signaling aggregation and routing, to overload handling, message parameter harmonization and load balancing.

The configuration settings are described in the topics listed below.

Topics:

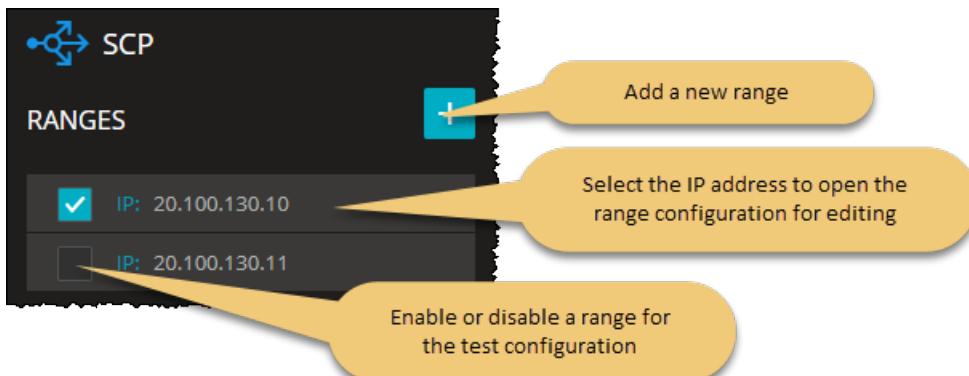
SCP Ranges panel	341
SCP Range panel	342
SCP interface settings	343
SCP Remote SBA Nodes	343

SCP Ranges panel

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

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

For example ...



SCP Range panel

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

- Select the **Delete Range** button to delete the selected SCP range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the SCP range.

SCP range controls and settings

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

The following table describes the available **Range** configuration options for each SCP 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 SCP is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the SCP functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	The SCP Node Settings are described below (Node Settings below).
SCP Interface Settings	Each SCP range requires the configuration of an interface necessary for SCP connectivity and use of indirect communication. These settings are described in SCP interface settings on the facing page .
Remote SBA Nodes	The remote SBA node settings are described in SCP Remote SBA Nodes on the facing page .

Node Settings

The following table describes the available SCP Node Settings.

Setting	Description
Instance ID	Each SCP instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
Forward to Another SCP	Select this check box to enable SCP Chaining. The SCP will be able to forward the messages it receives to a different SCP.
HTTP	The number of HTTP connections between two nodes.

Setting	Description
Connections	

SCP interface settings

The following **Connectivity Settings** enable the necessary SCP connectivity and use of indirect communication.

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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	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.

SCP Remote SBA Nodes

Peer SCP Type

Setting	Description
None	When this option is selected, the SCP chaining is not used.
Preset	Select this option in order to use a specific IP for next SCP hop.

Setting	Description
Discover	When this option is selected the SCP will send a request to NRF to discover the next hop SCP.

SCP Connection Settings

IMPORTANT These settings are available only when **Peer SCP Type** is set to **Preset**.

Setting	Description
Peer SCP	Select the IP address of the SCP node used as next hop.
Protocol	The protocol to use for communications. It can be either HTTP or HTTPS.
Port	The port number to use for communications. The default is port 80, but you can choose a different port number.

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

AUSF configuration settings



Authentication Server Function (AUSF) is the 5G core network service that handles authentication requests for 3GPP access and non-3GPP access networks. The AUSF serves as the termination point of user plane (UP) security, while providing the necessary authentication and authorization processes. It makes its services available to other network functions through the Nausf service-based interface. Multiple instances of AUSF may be deployed, with each instance storing specific data.

The configuration settings are described in the topics listed below.

Topics:

AUSF Ranges panel	346
AUSF Range panel	346
AUSF node settings	347
AUSF Nausf interface settings	348
AUSF remote SBA nodes	349

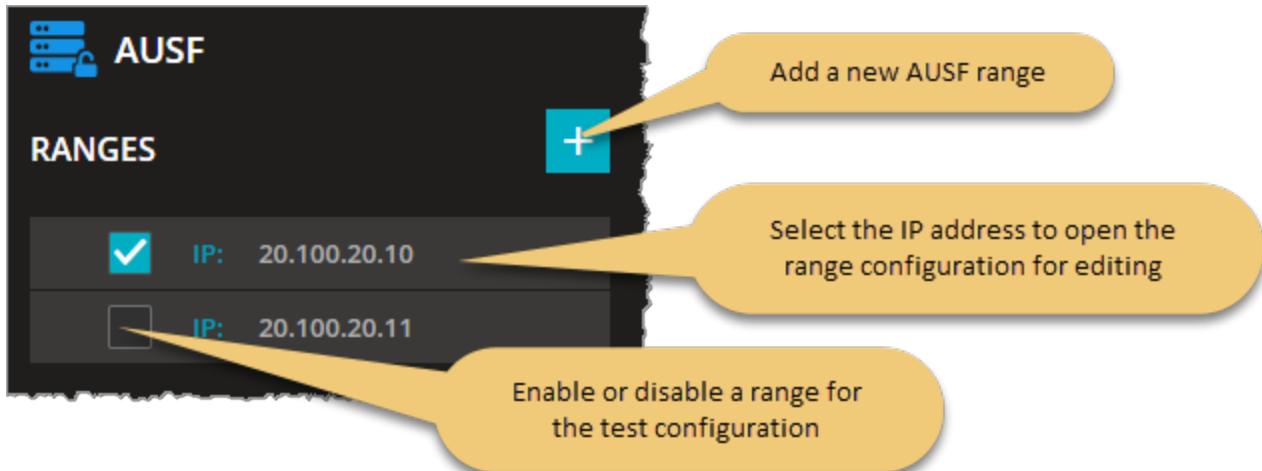
AUSF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



AUSF Range panel

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

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

AUSF range controls and settings

Each AUSF range is identified by a unique IP address. You can add and delete AUSF ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each AUSF 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 AUSF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the AUSF functionality (if

Setting	Description
	it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each AUSF range the configuration of an associated set of Node Settings, which are described in AUSF node settings below .
Nausf Interface Settings	Each AUSF range requires the configuration of Nausf interface settings, through which a AUSF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in AUSF Nausf interface settings on the next page .
Remote SBA Nodes	These settings are described in AUSF remote SBA nodes on page 349 .

AUSF node settings

Each AUSF range includes a set of Node Settings plus one or more associated Routing Indicators.

Node Settings

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

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

Routing Indicators

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.

You can add as many Routing Indicators as necessary to support your test objectives.

Setting	Description
	Select the Add Routing Indicator button to add a routing indicator for the AUSF range.
	Select the Delete button to remove the routing indicator from the AUSF range.

AUSF Nausf interface settings

Nausf is the service-based interface through which a AUSF instance makes its services available to other services in a 5G network.

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

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.

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

AUSF remote SBA nodes

UDM Connection Settings

To connect to the UDM node, the following configuration settings are required.

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> Select the IP address of the UDM node. This is the destination address of the UDM node to which the packets are sent over the Nudm interface. Select Discover to invoke the NF discovery service. <p>Refer to NF Discovery service on page 304 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nudm communications. It can be either HTTP or HTTPS.
Port	The UDM port number to use for Nudm communications. The default is port 80, but you can choose a different port number.
Use SCP Node	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the check box to enable it. For more details, refer to Use SCP.</p>

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.

Setting	Description
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

For several SBA nodes, if SCP is selected in SCP Connection Settings, a new option will be available:

- **Use SCP Node**

If SCP is selected in SCP Connection Settings, the messages will be forwarded to SCP on all the interfaces where SCP is supported. If **Use SCP Node** check box option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which the **Use SCP Node** check box is enabled will be forwarded to the SCP.

PCF configuration settings



Policy Control Function (PCF) is the 5G core network component that governs the network behavior by supporting unified policy framework. It provides policy rules to Control Plane function(s). This includes network slicing, roaming, and mobility management. Also, it accesses subscription information for policy decisions taken by the UDR. It makes its services available to other network functions through the Npcf service-based interface. Multiple instances of PCF may be deployed, with each instance storing specific data.

The configuration settings are described in the topics listed below.

Topics:

PCF Ranges panel	351
PCF Range panel	352
PCF node settings	353
PCF service area restrictions	353
PCF Npcf interface settings	355
PCF remote SBA nodes	356

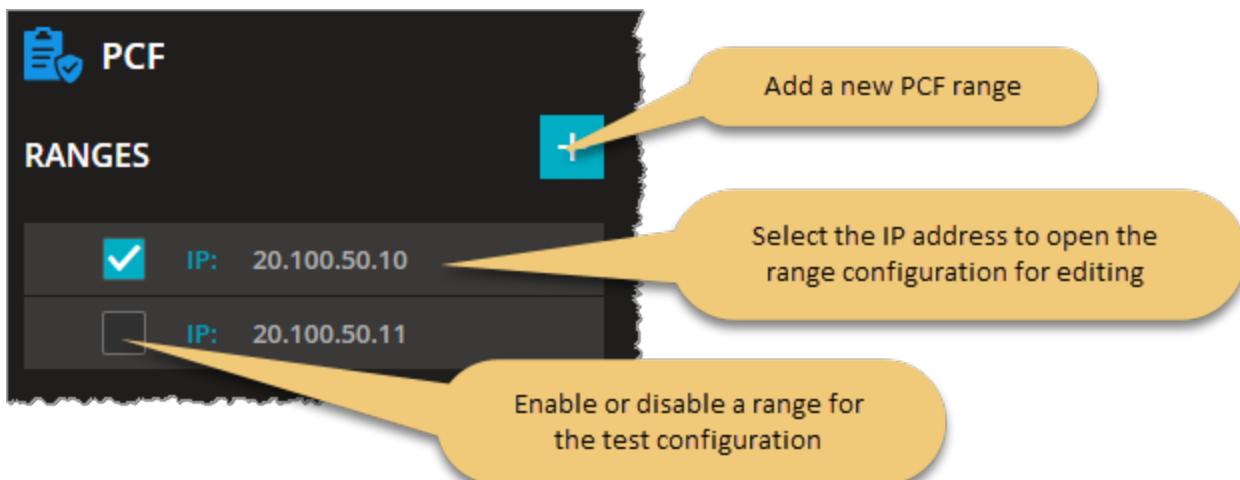
PCF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



PCF Range panel

You add and select PCF ranges from the PCF Ranges panel. When you select the IP address of an PCF node, LoadCore opens the **Range** panel, from which you can:

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

PCF range controls and settings

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

The following table describes the **Range Settings** that you configure for each PCF 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 PCF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the PCF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each PCF range the configuration of an associated set of Node Settings, which are described in PCF node settings on the facing page .
Service Area Restrictions	Each PCF range requires the configuration of the service area restrictions. The settings are described in PCF service area restrictions on the facing page .
Npcf Interface Settings	Each PCF range requires the configuration of Npcf interface settings, through which a PCF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in PCF Npcf interface settings on page 355 .
Remote SBA Nodes	These settings are described in PCF remote SBA nodes on page 356 .

PCF node settings

Each PCF range includes a set of Node Settings.

Node Settings

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

Setting	Description
Instance ID	<p>Multiple PCF instances may be deployed in the 5G network.</p> <p>Each PCF instance is uniquely identified by an <i>Instance ID</i>. You can accept the value provided by LoadCore or overwrite it with your own value.</p>
MCC	<p>The PLMN MCC for this PCF 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>
MNC	<p>The PLMN MNC for this PCF 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>
RFSP	The value of RAT/Frequency Selection Priority (RFSP) index.
Triggers	<p>Request Triggers to which the PCF subscribes. The allowed values are:</p> <ul style="list-style-type: none"> • Location Change (tracking area). The tracking area of the UE has changed. • PRA Change (change of UE presence in PRA). The UE is entering/leaving a Presence Reporting Area. <p>Both values can be selected simultaneously.</p>
Include Request in Response	Select the check-box to include the request in the response message.

PCF service area restrictions

The policy information sent from the PCF to AMF may contain service area restrictions for the UE. This means that the UE's access to the network resources can be restricted or limited.

The following configuration settings are required in order to define service area restrictions.

Setting	Description
<i>Service Area Restrictions:</i>	
Restriction type	<p>Set the restriction type attribute:</p> <ul style="list-style-type: none"> • Allowed Areas • Not Allowed Areas
Max No. Of TAs	The maximum number of allowed TAs that can be traversed.

The following configuration settings are required in order to define the tracking area identities.

For each PCF range in your test configuration, you can add and delete AREAS as required to meet your test objectives.

Setting	Description
<i>Areas:</i>	
	Select the Add Area button to add a new restriction area to your configuration.
<i>Area:</i>	
	Select the Delete Area button to remove the restriction area from your configuration.
Area Codes	<p>Set the area code.</p> <p>Location Area Code (LAC) is a fixed length code (two octets) identifying a location area within a PLMN.</p>
<i>TACS:</i>	
	<p>This represents the Tracking Area Code (TAC) for this eNodeB. Select the Add TAC button to add a new TAC to your configuration.</p> <p>A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).</p>
	Select the Delete button to remove the tracking area code from your configuration.

After configuring it, the Service Area Restriction information consists of:

- either:
 - the maximum number of allowed TAs that can be traversed encoded as Max No. Of TAs attribute, and/or
 - both of :
 - a list of allowed Tracking Area Identities (TAIs) encoded as TACS attributes within the AREA attribute
 - the restriction type attribute set to Allowed Areas
- or:
 - a list of not allowed Tracking Area Identities (TAIs) encoded as TACS attributes within the AREA attribute, and
 - the restriction type attribute set to Not Allowed Areas

PCF Npcf interface settings

Npcf is the service-based interface through which a PCF instance makes its services available to other services in a 5G network. The following **Connectivity Settings** enable the necessary Npcf connectivity and service interaction.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
<i>Outer VLAN</i>	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.

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

PCF remote SBA nodes

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

UDR configuration settings



Unified Data Repository (UDR) is the 5G core network service that maintains a repository of data that can be used by a number of 5G network functions. For example, the UDR may store subscription data that is used by the UDM and policy data that is used by the PCF. It makes its services available to other network functions through the Nudr service-based interface. Multiple instances of UDR may be deployed, with each instance storing specific data or providing service to a specific set of network function (NF) consumers.

The configuration settings are described in the topics listed below.

Topics:

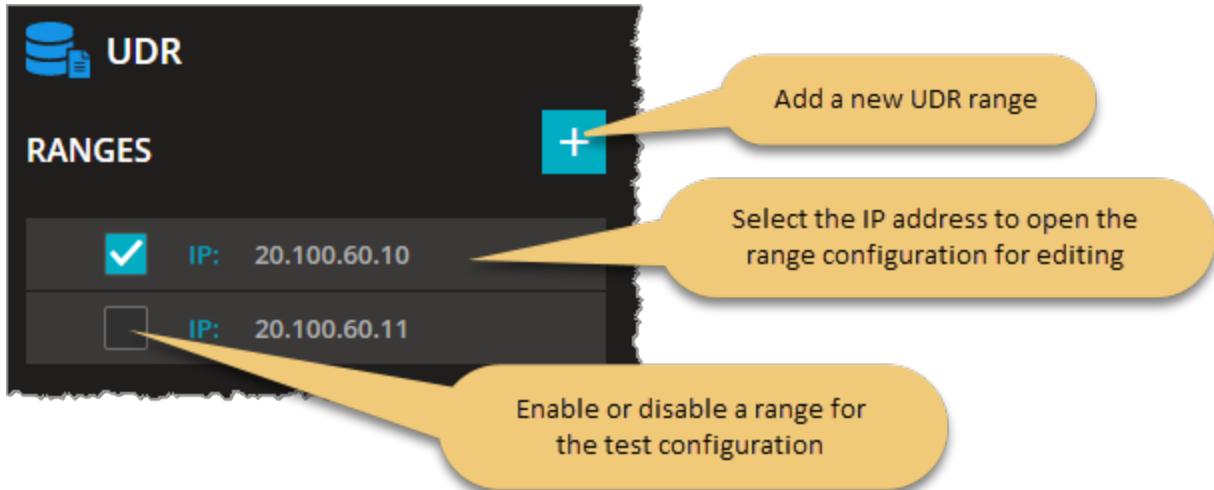
UDR Ranges panel	356
UDR Range panel	357
UDR Nudr interface settings	358
UDR remote SBA nodes	359

UDR Ranges panel

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

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

For example ...



UDR Range panel

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

- Select the **Delete Range** button to delete the selected UDR range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node and connectivity settings for the UDR range.

UDR range controls and settings

Each UDR range is identified by a unique IP address. You can add and delete UDR ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each UDR 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 UDR is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the UDR functionality (if it is selected in the Topology window).
<i>Node Settings:</i>	
Instance ID	Multiple UDR instances may be deployed in the 5G network, with each one storing specific data or providing service to a specific set of NF consumers.

Setting	Description
	Each UDR instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
Nudr Interface Settings	Each UDR range requires the configuration of Nudr interface settings, through which a UDR instance enables connectivity and interaction with other functions in the 5G network. These settings are described in UDR Nudr interface settings below .
Remote SBA Nodes	These settings are described in UDR remote SBA nodes on the facing page .

UDR Nudr interface settings

Nudr is the service-based interface through which a UDR instance makes its services available to other services in a 5G network. The following **Connectivity Settings** enable the necessary Nudr connectivity and service interaction.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT 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>

Connectivity Settings	Description
VLAN ID	VLAN identifier.

UDR remote SBA nodes

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

UDM configuration settings



Unified Data Management (UDM) is the 5G core network service that is responsible for a number of functions, including the generation of AKA authentication credentials, user identification handling, access authorization, subscription management, among others. It makes its services available to other network functions through the Nudm service-based interface. Multiple instances of UDM may be deployed. A UDM Group ID refers to one or more UDM instances managing a specific set of SUPIs.

The configuration settings are described in the topics listed below.

Topics:

UDM Ranges panel	359
UDM Range panel	360
UDM node settings	361
UDM Nudm interface settings	364
UDM remote SBA nodes	365

UDM Ranges panel

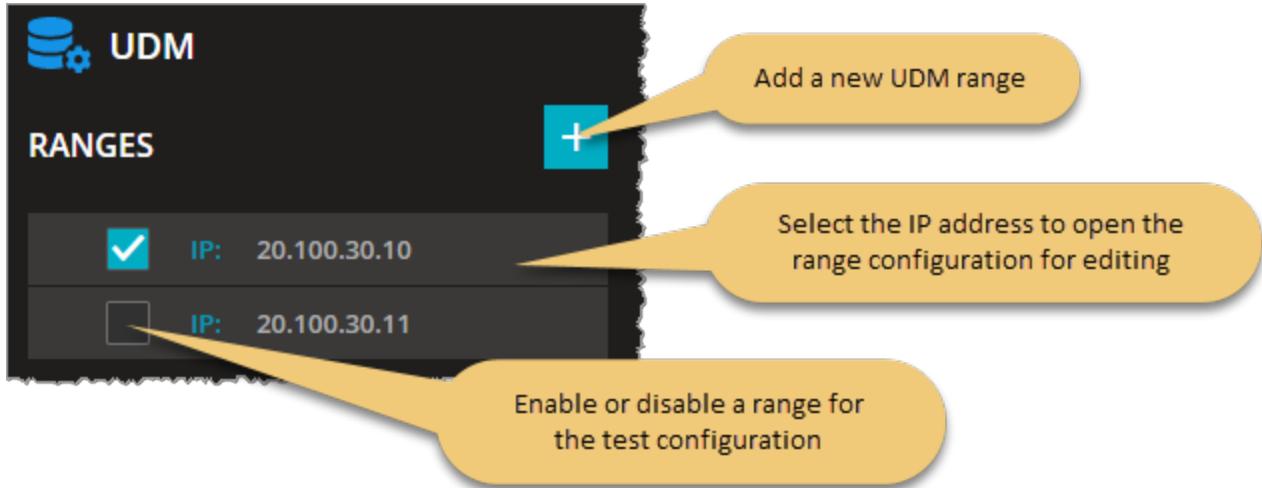
The **UDM Ranges** panel opens when you select the UDM node from the network topology window.

You can perform the following tasks from this panel:

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

- Enable or disable a range for the test configuration.

For example ...



UDM Range panel

You add and select UDM ranges from the UDM Ranges panel. When you select the IP address of a UDM, LoadCore opens the **Range** panel, from which you can:

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

UDM range controls and settings

Each UDM range is identified by a unique IP address. You can add and delete UDM ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each UDM 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 UDM is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the UDM functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each UDM range requires the configuration of an associated set of Node Settings, which are described in UDM node settings on the facing page .
Nudm Interface	Each UDM range requires the configuration of Nudm interface settings, through

Setting	Description
Settings	which a UDM instance enables connectivity and interaction with other functions in the 5G network. These settings are described in UDM Nudm interface settings on page 364 .
Remote SBA Nodes	These settings are described in UDM remote SBA nodes on page 365 .

UDM node settings

Each UDM range includes a set of Node Settings plus one or more associated Routing Indicators.

Node Settings

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

Setting	Description
Instance ID	The Instance ID uniquely identifies each UDM instance. You can accept the value provided by LoadCore or overwrite it with your own value.
MCC	<p>The PLMN MCC for this UDM 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>
MNC	<p>The PLMN MNC for this UDM 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>
Home Network Private key	<p>The Home Network Private key that is used for subscriber privacy.</p> <p>The Subscription identifier de-concealing function (SIDF)—which is a service provided by the UDM—is responsible for de-concealing the SUPI from the SUCI. When the Home Network Public Key is used for encryption of the SUPI, the SIDF uses the Home Network Private Key that is securely stored in the home operator's network to decrypt the SUCI. The de-concealment takes place at the UDM. Access rights to the SIDF are defined such that only a network element of the home network is allowed to request SIDF.</p>

Setting	Description
	<p>Note that one UDM can comprise several UDM instances. The Routing Indicator in the SUCI can be used to identify the specific UDM instance that is capable of serving a subscriber.</p> <p>About SUPI and SUCI ... The Subscription Permanent Identifier (SUPI) is a globally unique identifier allocated to each subscriber in the 5G System. The Subscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed SUPI.</p>

Routing Indicators

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.

You can add as many Routing Indicators as necessary to support your test objectives.

Setting	Description
	Select the Add Routing Indicator button to add a Routing Indicator for the UDM range.
	Select the Delete button to remove the routing indicator from the UDM range.

SDM Notifications

The UDM is a database-like Network Function(NF). It keeps information about the subscribers (users). The information about a subscriber is organized as a collection of resources corresponding to that user (*nssai*, *am-data*, *sm-data*, *smf-select-data* etc). A resource is a JSON object, containing sub-objects identified by a path.

When other Network Functions (NFs) register to UDM for a certain subscriber, they get some of those resources (for that specific user) and also ask the UDM to subscribe for changes to those resources (so for example, through a subscription operation, the AMF requests from the UDM a notification when *am-data* resource for this user changes).

Basically, through the SDM Notifications, UDM is delivering notifications to other interested NFs about changes to its resources.

The SDM Notifications defines a list of resources and the changes that occur for each of those resources

You can add as many SDM notification subscriptions as necessary to support your test objectives. To do this, select the **Add UDM Triggered SDM Notifications Table** button.

The following table describes the parameters that you need to configure for each SDM subscription.

Setting	Description
<i>SDM Subscription:</i>	

Setting	Description
	Select the Delete Subscription button to remove this subscription from the SDM notifications.
Resource name	This represents the subscribed resource (entered as a string) for which notifications are triggered. Valid strings currently supported: <i>nssai, am-data, smf-select-data, sm-data, ue-context-in-smf-data</i> .
Notification trigger time (ms)	This represents the time interval (in milliseconds) from NF subscription (for that resource) after which that NF will start receiving notifications from UDM.
Change resource continuously	Select this option to apply the changes from the list continuously(start over again when reaching the end of the list). If this option is not selected, the notifications for the resource will stop when the last change in the list will happen, otherwise they will start from the beginning again.
<i>Resource changes:</i>	
	Select the Add change button to add new list of changes that will happen over time to the defined resource.
<i>Change Item</i>	
	Select the Delete Change Item to remove this list from your configuration.
Change type	This represents the nature of the change: <ul style="list-style-type: none"> • Add - new content was added to the resource. • Change - a certain content has changed. • Remove - a certain content was removed. • Move - a certain content has been moved from one place to another.
Path in resource to change	The resource is a JSON object and it is comprised of multiple JSON sub-objects. This path describes which sub-object will be the target of the change (if left empty, it designated the resource object).
New JSON value	This represents the new JSON text value for the object identifier by the Path in resource to change . <div style="background-color: #005a7b; color: white; padding: 2px 10px; margin-left: 10px;">IMPORTANT</div> This field must have a valid JSON text value only if the Change type is set to Add or Replace .
Trigger after previous notification change (ms)	This represents the time interval starting from the previous change notification, after which this notification should be delivered. The first notification would not use this value, it will be delivered using the value of Notification Trigger timer .

Setting	Description
From source path (used for Move change type)	<p>NOTE This parameter is available only when Change type is set to Move. This represents the original path of the JSON object that has been moved.</p>

UDM Nudm interface settings

Nudm is the service-based interface through which a UDM instance makes its services available to other services in a 5G network.

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

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT 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.

UDM remote SBA nodes

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

CHF configuration settings



The Charging Function (CHF) allows charging services to be offered to authorized network functions. Policy and Charging Control plays a very critical role in the 5G ecosystem. It provides control and transparency over the consumption of Network resources during real-time service delivery.

The PCF (Policy Charging Function) governs the Control plane functions via Policy rules defined and User plane functions via Policy enforcement. It works very closely with CHF (Charging Function) for Usage Monitoring.

In the SBA test topology, the charging function is used to test PCF. As a result, PCF must act as the device under test(the set the PCF as a DUT refer to [PCF range controls and settings](#)).

The configuration settings are described in the topics listed below.

Topics:

CHF Ranges panel	366
CHF Range panel	366
CHF node settings	367
CHF Nchf interface settings	367
CHF remote SBA nodes	368

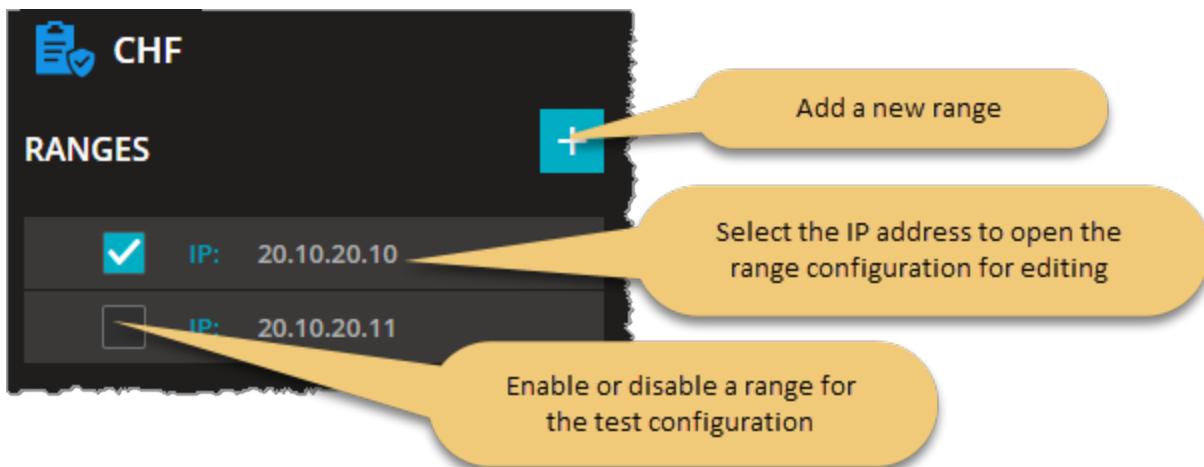
CHF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



CHF Range panel

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

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

CHF range controls and settings

Each CHF range is identified by a unique IP address. You can add and delete CHF ranges as necessary to support your test objectives. The following table describes the available **Range** configuration options for each CHF 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 CHF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the CHF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each CHF range includes a set of Node Settings, which are described in CHF node settings below .
Nchf Interface Settings	Each CHF range requires the configuration of Nchf interface settings, through which a CHF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in CHF Nchf interface settings below .
Remote SBA Nodes	These settings are described in CHF remote SBA nodes on the next page .

CHF node settings

Each CHF range includes a set of Node Settings.

Node Settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	The Instance ID uniquely identifies each CHF instance. You can accept the value provided by LoadCore or overwrite it with your own value.

CHF Nchf interface settings

Nchf is the service-based interface through which a CHF instance makes its services available to other services in a 5G network.

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

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

Connectivity Settings	Description
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).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

CHF remote SBA nodes

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

NSSF configuration settings



The Network Slice Selection Function (NSSF) selects Network Slice Instances (NSIs) based on information provided during UE attach. The NSSF offers services to the AMF (and to NSSFs to different PLMNs) via the Nnssf service based interface.

N22 is the reference point between AMF and NSSF, and N31 is the reference point between the NSSF in the visited network and the NSSF in the home network.

The NSSF supports the following functionality:

- Selecting the set of Network Slice instances serving the UE
- Determining the Allowed NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs
- Determining the Configured NSSAI and, if needed, the mapping to the Subscribed S-NSSAIs
- Determining the AMF Set to be used to serve the UE

Topics:

NSSF Ranges panel	371
NSSF Range panel	371
NSSF node settings	372
Nnssf Interface Settings	373
Remote SBA nodes	374
NSSF Restricted NSSAIs	375
NSSF Network Slices	376
NSSF Configured NSSAI	377

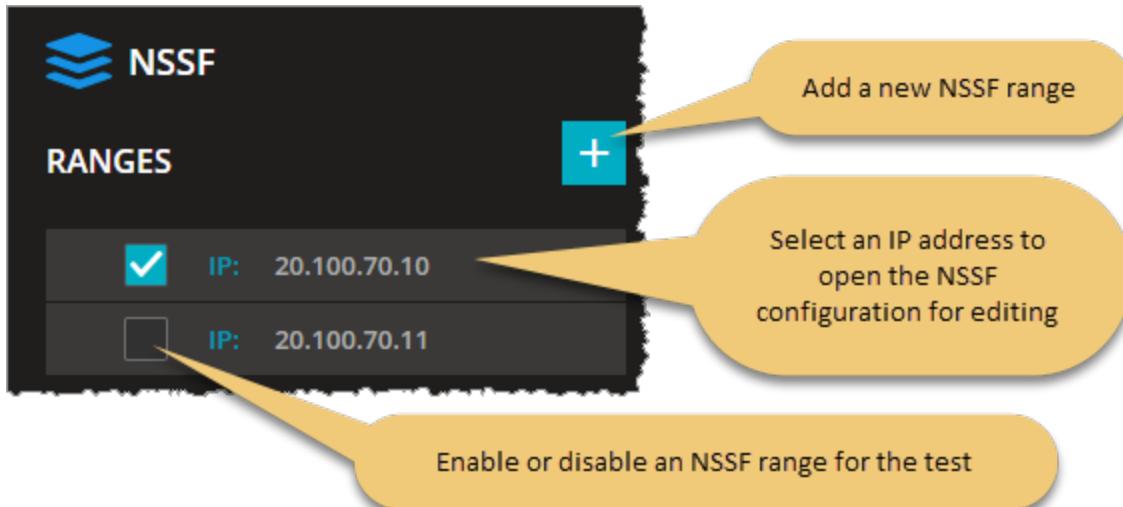
NSSF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



NSSF Range panel

Selecting an IP address from the NSSF **Ranges** panel provides access to the configuration settings on the **Range** panel. From the NSSF **Range** panel, you can:

- Delete the NSSF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Select **Range Settings** to configure the node, Nnssf interface, and remote SBA nodes.
- Select **Network Slicing** to configure restricted NSSAIs, network slices, and configured NSSAIs.

NSSF range controls and settings

Each NSSF range is identified by a unique IP address. You can add and delete NSSF ranges as necessary to support your test requirements. The following table describes the **Range Settings** that you need to configure for each NSSF range.

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

Setting	Description
Device Under Test	Enable this option if your NSSF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the NSSF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each NSSF range requires the configuration of an associated set of Node Settings, which are described in NSSF node settings below .
Nnssf Interface Settings	Each NSSF range requires the configuration of Nnssf interface settings, through which a NSSF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in Nnssf Interface Settings on the facing page .
Remote SBA Nodes	These settings are described in Remote SBA nodes on page 374 .
<i>Network Slicing:</i>	
Restricted NSSAIs	These settings are described in NSSF Restricted NSSAIs on page 375 .
Network Slices	These settings are described in NSSF Network Slices on page 376 .
Configured NSSAIs	These settings are described in NSSF Configured NSSAI on page 377 .

NSSF node settings

Each NSSF range includes a set of Node Settings. Each NSSF instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple NSSF instances may be deployed in the 5G network. Each NSSF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
PLMN MCC	Set the mobile country code. About PLMN MCC ... A Public Land Mobile Network (PLMN) is a telecommunications network that provides

Setting	Description
	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	Set the mobile network code. 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 Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.

Nnssf Interface Settings

Nnssf is the service-based interface through which an NSSF instance makes its services available to other services in a 5G network.

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

Connectivity Setting	Description
<i>IP:</i>	
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The length of the IP prefix for this interface.
Gateway Address	The gateway address through which other servers will access this NSSF instance.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
<i>Outer VLAN:</i>	
Outer VLAN	Enable this option if you are using VLANs on this interface.

Connectivity Setting	Description
VLAN ID	The outer VLAN identifier.
<i>Inner VLAN:</i>	
Inner VLAN	Enable this option if you are using VLANs on this interface and you need to configure inner VLANs. The Inner VLAN configuration settings are available only when <i>Outer VLAN</i> is enabled.
VLAN ID	The inner VLAN identifier.

Remote SBA nodes

NRF Connection Settings

To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

Setting	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select either the IP address of an NRF from your test network or <i>None</i> if you are not using an NRF in your test configuration. The IP address is the destination address of the NRF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnrf communications. It can be either HTTP or HTTPS.
Port	The port number to use for Nnrf communications. The default is port 80, but you can choose a different port number.

SCP Connection Settings

To connect to the Service Communication Proxy (SCP) node, the following configuration settings are required.

Setting	Description
<i>SCP Connection Settings:</i>	
Peer SCP	Select either the IP address of an SCP from your test network or <i>None</i> if you are not using an SCP in your test configuration. The IP address is the destination address of the SCP node to which the packets are sent for Indirect Communication.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.

NSSF Restricted NSSAIs

The AMF uses the NSSAI Availability Service to update the S-NSSAIs that the AMF supports on a per-TA basis on the NSSF and to subscribe and notify any status changes, on a per-TA basis, of the S-NSSAIs available per TA (unrestricted) and the restricted S-NSSAI(s) per PLMN in that TA in the serving PLMN of the UE.

You use the **NSSF Restricted NSSAIs** settings to define the Restricted NSSAIs for your test. For each Restricted NSSAI in your configuration, you will configure one or more Restricted S-NSSAIs.

Setting	Description
<i>Restricted NSSAIs:</i>	
	Select the Add a restricted NSSAI button to add a restricted NSSAI to your test configuration.
<i>Restricted NSSAI settings:</i>	
	Select the Delete Restricted NSSAI button to delete this NSSAI from your test configuration.
<i>Tracking Area Identity (TAI):</i>	
MCC	The PLMN MCC that is used in the construction of this TAI.
MNC	The PLMN MNC that is used in the construction of this TAI.
TAC	The PLMN TAC that is used in the construction of this TAI.
<i>Restricted S-NSSAIs:</i>	
	Select the Add NSSAI button to add a Restricted A-NSSAI to your test configuration.
<i>NSSAI Settings:</i>	
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default 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 default Mapped configure Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The default Mapped configured Slice Differentiator (SD) value for this S-NSSAI.

NSSF Network Slices

You use the **NSSF Network Slices** settings to configure one or more network slices for use in your test. A network slice is a 5G logical network that provides specific network capabilities and network characteristics.

Setting	Description
<i>Network Slices:</i>	
	Select the Add a Network slice button to add a network slice to your test configuration.
<i>Network Slice settings:</i>	
	Select the Delete a Network Slice button to remove this network slice from your test configuration.
Slice Name	Each network slice is uniquely identified by a <i>Slice Name</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Slice NRF (Network Repository Function):</i>	
Slice NRF host	The identifier (IP address) of the Network Repository Function (NRF) host to be used to select services within a Network Slice instance.
Protocol	The protocol used for communications. You can choose either HTTP or HTTPS.
Port	The port number used for communications. The default is port 80, but you can choose a different port number.
<i>Tracking Areas:</i>	
	Select the Add Tracking Area button to add a Tracking Area (TA) to your test configuration.
<i>Tracking Area Indication (TAI) settings:</i>	
	Select the Delete TAI button to delete this TAI from your test configuration.
MCC	The Mobile Country Code (MCC) used in the construction of the TAI.
MNC	The Mobile Network Code (MNC) used in the construction of the TAI.
TAC	The Tracking Area Code (TAC) used in the construction of the TAI.

NSSF Configured NSSAI

You use the **NSSF Configured NSSAI** settings to define one or more Configured NSSAIs for your test configuration. A Configured NSSAI is an NSSAI with which the PLMN may configure a UE, in which case the UE will use it as the default NSSAI.

Setting	Description
<i>Configured NSSAI:</i>	
	Select the Add a Configured NSSAI button to add a Configured NSSAI to your test configuration.
<i>Configured SNSSAI settings:</i>	
	Select the Delete a Configured NSSAI button to remove this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The default Mapped configured Slice/Service Type (SST) value for this NSSAI.
Mapped SD	The default Mapped configured Slice Differentiator (SD) value for this NSSAI.
Slice names	Select from among the available slice names (the slices that you defined using the NSSF Network Slices settings). There is also an option to select all of the slices.

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:

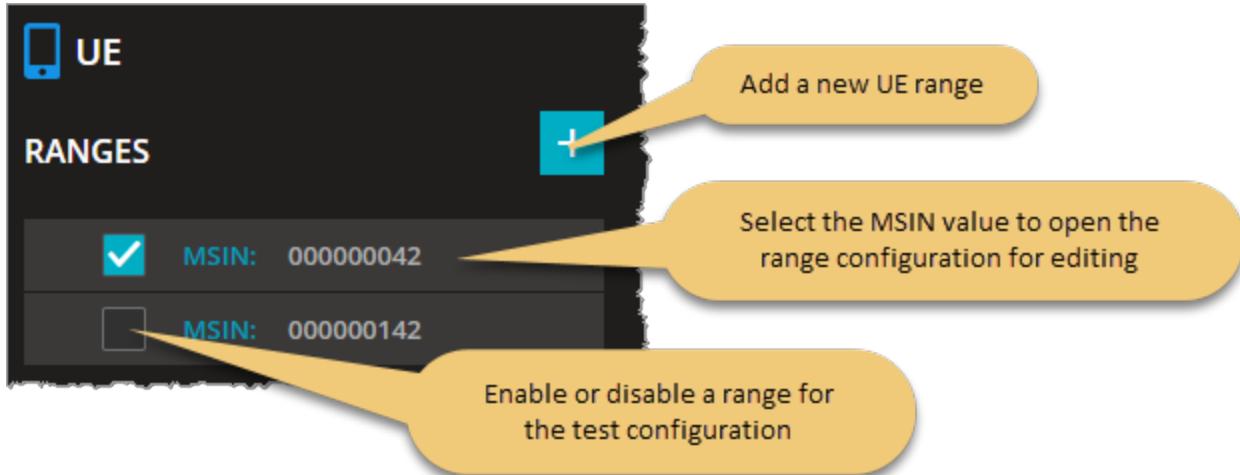
UE Ranges panel	379
UE Range panel	379
Range Settings	380
UE Identification	381
UE Security	381
UE Settings	383
UE SDF settings	384
Shared Data IDs	385
UE Subscribed AMBR settings	385
Service Area Restrictions	385
Forbidden Areas	386
Notifications	387
Network Slicing	388
UDM Default NSSAI settings	389
UDM SNSSAI Mappings	389
UDR SNSSAI Settings	390
Charging Function	390
Policy Counters	391
Notify Policy Counters	392

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, LoadCore opens the **Range** panel, from which you can:

- Delete the UE range from the test configuration.
- Configure the *Range Count*.
- Access the detailed UE configuration settings (Range Settings, Network Slicing, Objectives).

UE range controls and settings

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.

Detailed UE configuration settings

The Range panel also provides links to the detailed configuration settings:

- [Range Settings below](#)
- [Network Slicing on page 388](#)
- [Objectives on page 394](#)

Range Settings

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

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

- [UE Identification on the facing page](#)
- [UE Security on the facing page](#)
- [UE Settings on page 383](#)
- [UE SDF settings on page 384](#)
- [Shared Data IDs on page 385](#)
- [UE Subscribed AMBR settings on page 385](#)
- [Service Area Restrictions on page 385](#)
- [Forbidden Areas on page 386](#)

UE Identification

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
MCC	The MCC that will be assigned to each UE in this range.
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 SV	The IMEI SV value that will be assigned to the first simulated UE in the range.
IMEI SV increment	The value to use for incrementing the IMEISV values for each of the UEs in the range.
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 IP Address	The IPv4 address that has been assigned to the first simulated UE in the range.
UE IP increment	The value to use for incrementing the IPv4 addresses for each of the UEs in the range.
UE IPv6 Address Prefix	The IPv6 address prefix that has been assigned to the first simulated UE in the range.
UE IPv6 Address Prefix Increment	The value to use for incrementing the IPv6 address prefixes for each of the UEs in the range.
UE IPv6 Address Prefix Length	The IPv6 address prefix that has been assigned to the UEs in the range.

UE Security

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 LoadCore, 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 LoadCore, 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 LoadCore, 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.
RAND	A hexadecimal number that represents the 128-bit random challenge. You can accept the value generated by LoadCore, or enter of a RAND value of your own choosing.
AUTN	The AUthentication TokeN (AUTN) to use when authenticating the UEs in this range.
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:

Setting	Description		
	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 used 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	The Routing Indicator that is used in the construction of the SUCI. The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.		
Authentication Type	Select the Authentication Method to use in the authentication procedures for this range of UEs. In the current release, 5G-AKA is the only supported Authentication Type.		

UE Settings

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

Setting	Description
<i>Settings:</i>	
Allow MICO Mode	This option, when selected, indicates that the UEs in the range prefer Mobile Initiated Connection Only (MICO) mode during Initial Registration and Registration Update procedures.
Subscribed Registration	The Periodic Registration timer value for this range of UEs. The AMF allocates a periodic registration timer value to the UE based on local policies, subscription

Setting	Description
Timer	information and information provided by the UE. After the expiry of this timer, the UE performs a periodic registration.
Active Time	The subscribed Active Time for Power Saving Mode (PSM) UEs.
RAT Restrictions	UE Mobility Restrictions include RAT restrictions, which define the 3GPP Radio Access Technologies (one or more) that a UE is not allowed to access in a PLMN. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual.
Wake Up Timer 5G To 4G	The time interval (in seconds) to elapse from UDM initiated deregistration (5G to 4G) until the user is restarted.
<i>Access and Mobility Policy:</i>	
Subscription Categories	Select the desired Subscription Category for this range of UEs. <i>Subscriber Category</i> 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).

UE SDF settings

Each UE range has a set of **SDF** settings that configure subscription Service Data Flow values for the PDU sessions in the range.

Setting	Description
<i>SDF Settings:</i>	
UE UDP Port	The starting client-side UDP port number for the Service Data Flows (SDFs) in the PDU session.
UE UDP Port Increment	The value by which the client-side UDP port numbers are incremented for the SDFs in the PDU session.
Layer 7 Server IP	The starting IP address of the destination server for the SDFs in the PDU session.
Layer 7 Server IP Increment	The value by which the server IP addresses are incremented for the SDFs in the PDU session.
Layer 7 Server UDP Port	The server-side UDP port number for the SDFs in the PDU session.
Layer 7 Server UDP Port Increment	The value by which the server-side UDP port numbers are incremented for the SDFs in the PDU session.

Shared Data IDs

You use the **Shared Data ID** panel to create a list of shared-data-ids. These IDs are used to request the shared-data resources from the UDM.

A UE subscription may contain both individual subscription data and shared subscription data (subscription data that is shared by multiple UEs). These shared data are identified by Shared Data IDs that are listed in the UE individual data.

Use the **Add ID** button to add additional IDs to the list, and the **Delete ID** button to removed IDs from the list.

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 Session-AMBR value for this range of UEs.
Subscribed AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Subscribed AMBR Downlink	The subscribed downlink Session-AMBR value for this range of UEs.
Subscribed AMBR Downlink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.

Service Area Restrictions

A UE subscription may contain service area restrictions, which place limits on the areas in which the UE may initiate communication with the network. A Service Area Restriction definition consists of either a list of allowed Tracking Area Identities (TAIs) or a list of non-allowed TAIs and, optionally, specifies the maximum number of allowed TAIs.

You use the settings described below to configure service area restrictions for a UE range (these configuration settings are also made available on the UDM). You can add and delete service area restriction Areas for the UE range as needed to meet your test requirements.

Service Area Restrictions

Setting	Description
Restriction Type	<p>The type of restriction to use for this range of UEs. It is either Not Allowed Areas or Allowed Areas.</p> <p>The list of allowed TAIs indicates the TAIs where the UE is allowed to be registered, and the list of non-allowed TAIs indicates the TAIs where the UE is not allowed to be registered.</p> <p>A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed</p>

Setting	Description
	from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).
Max No. of TAs	The maximum number of allowed TAIs for this UE range.

Areas

Each Service Area Restriction specifies one or more Areas (Allowed or Not Allowed Areas), each of which contains a list of TACs. You can add and delete areas from the Service Area Restrictions settings as needed to meet your test requirements.

Setting	Description
<i>Areas:</i>	
	Select the Add Area button to add a new restriction area to your configuration.
<i>Area:</i>	
	Select the Delete Area button to remove the restriction area from your configuration.
Area Codes	Each Area that you configure is identified by an Area Code, which is an operator-specific string value.
<i>TACs:</i>	
	Select the Add TAC button to add a new TAC to your configuration. Each Area that you add to a UE range's Service Area Restriction contains a list of one or more TACs. A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).
	Select the Delete button to remove the tracking area code from your configuration.

Forbidden Areas

A UE subscription may include a list of Forbidden Areas. In a Forbidden Area, the UE is not permitted to initiate any communication with the network.

You use the settings described below to configure forbidden areas for a UE range (these configuration settings are also made available on the UDM). You can add and delete Forbidden Areas for the UE

range as needed to meet your test requirements.

Setting	Description
<i>Forbidden Area:</i>	
	Select the Delete Forbidden Area button to remove this area from your configuration.
Area Codes	Each Area that you configure is identified by an Area Code, which is an operator-specific string value.
<i>TACs:</i>	
	Select the Delete button to remove this TAC from your configuration.
TAC	<p>Each Area that you add to a UE range's Forbidden Area contains a list of one or more TACs.</p> <p>A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).</p>

Notifications

Each UE range in the SBA topology has a set of **Notifications** values that configure Unified Data Repository (UDR) notifications for the range.

The UDR stores policy data that is used by the network service consumers (PCF, UDM, and NEF). Among the functionalities supported by the UDR is subscriptions to notification and the notification of subscribed data changes.

Setting	Description
<i>UDR Notifications:</i>	
Delay in milliseconds	The delay in milliseconds between Policy Data Subscriptions and Policy Data Change Notification.
<i>Policy Data:</i>	
Enable notification	Enable subscription to policy data notifications for the UE range.
SM Policy Data json	Paste your policy data JSON file into the field.
<i>Application Data:</i>	
Enable	Enable subscription to application data notifications for the UE range.

Setting	Description
notification	
Application Data json	Paste your application data JSON file into the field.

Network Slicing

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:

UDM Default NSSAI settings	389
UDM SNSSAI Mappings	389
UDR SNSSAI Settings	390

UDM Default NSSAI settings

You can add and delete UDM Default SNSSAI settings as required to meet your test objectives.

A UE Registration Request will include the Default Configured NSSAI Indication if the UE is using a Default Configured NSSAI. The Default Configured NSSAI, when configured in the UE, is used by the UE in a Serving PLMN only if the UE has no Configured NSSAI for the Serving PLMN.

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

Setting	Description
<i>UDM Default NSSAI:</i>	
	Select the Add UDM Default NSSAI button to add the default NSSAI to your test configuration.
<i>UDM Default NSSAI settings:</i>	
	Select the Delete UDM Default NSSAI button to delete this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this S-NSSAI.
Mapped SST	The default Mapped configure Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The default 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.

Setting	Description
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 one or more DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .

UDR SNSSAI Settings

The following table describes the UE **UDR SNSSAI** settings.

Setting	Description
<i>UDR SNSSAI Settings:</i>	
	Select the Add SNSSAI Settings button to add the SNSSAI settings to your test configuration.
<i>UDR Settings:</i>	
	Select the Delete SNSSAI Settings button to delete this SNSSAI settings configuration from your test configuration.
SST	The Slice/Service Type (SST) value
SD	The Slice Differentiator (SD) value for this SNSSAI. 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 Slice/Service Type (SST) value for this SNSSAI.
Mapped SD	The Mapped Slice Differentiator (SD) value for this SNSSAI.
DNNS	A DNN (Data Network Name) with which PDU sessions will be associated for this SNSSAI. Select one or more DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .

Charging Function

At this point, LoadCore's Charging Function supports only Spending Limit Control.

The Spending Limit Control Service is provided by the Charging Function (CHF) and enables the NF service consumer to retrieve policy counter status information. The internal CHF functionality for policy counter management provisioning is specified in 3GPP TS 32.240.

The following table describes the UE **Spending Limit Control** settings.

Setting	Description
Enable Notify Timer	Select this option to activate the notify timer.
Trigger Notify Timer(ms)	The time interval (in milliseconds) after which CHF will notify PCF with modified policy counters.
Enable Subscription Termination Timer	Select this option to activate the subscription termination timer.
Trigger Subscription Termination (ms)	The time interval (in milliseconds) after which CHF will request PCF to terminate a subscription.
Supported Features	Policy label.
Policy Counters	For more details about DNN configuration, refer to Policy Counters below .
Notify Policy Counters	For more details about DNN configuration, refer to Notify Policy Counters on the next page .

Policy Counters

The following table describes the **Policy Counters** settings.

Setting	Description
<i>Policy Counters:</i>	
	Select the Add Policy Counter button to add a policy counter to your test configuration.
<i>Policy Counter settings:</i>	
	Select the Delete Policy Counter button to delete this policy from your test configuration.
Policy Counter Id	This parameter is used to identify a policy counter. You can accept the value provided by LoadCore or overwrite it with your own value.
Current Status	Enter the policy counter status (as a string value). For example: <i>100Mbps</i> .
<i>Pending Statuses:</i>	
	Select the Add Pending Status button to add a pending policy counter status.

Setting	Description
<i>Pending Policy Counter Status settings:</i>	
	Select the Delete Pending Policy Counter Status button to remove the pending policy counter status.
Policy Counter Status	Enter the pending policy counter status (as a string value). For example: <i>100Mbps</i> .
Activation Time	Enter the activation time (as a DateTime value) for this pending status value. For example: <i>2020-12-31 11:59:59</i> .

Notify Policy Counters

The Policy Counters notifications are messages sent by CHF whenever the policy status has changed and contain the new policy status.

The notifications are enabled only after the **Enable Notify Timer** option is selected and will be sent based on the time interval set for the **Trigger Notify Timer (ms)** parameter.

The following table describes the **Notify Policy Counters** settings.

Setting	Description
<i>Policy Counters:</i>	
	Select the Add Policy Counter button to add a policy counter to your test configuration for which you want to receive notifications.
<i>Policy Counter settings:</i>	
	Select the Delete Policy Counter button to delete this policy from your test configuration.
Policy Counter Id	This parameter is used to identify the policy counter for which to receive notifications.
Current Status	Enter the policy counter current status (as a string value). For example: <i>120Mbps</i> .
<i>Pending Statuses:</i>	
	Select the Add Pending Status button to add a pending policy counter status.
<i>Pending Policy Counter Status settings:</i>	
	Select the Delete Pending Policy Counter Status button to remove the pending policy counter status.
Policy	Enter the policy counter status (as a string value). For example: <i>120Mbps</i> .

Setting	Description
Counter Status	
Activation Time	Enter the activation time (as a DateTime value) for this status value. For example: 2020-12-31 11:59:59.

Objectives

In a LoadCore test, an *objective* is a set of performance or 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:

Primary Objective	395
About primary objectives	396
Active subscribers	398
Subscribers per Second	403
Secondary Objectives	408
UEGetNSSAIAMF2UDM	409
RegistrationAMF2UDM	410
DeregistrationAMF2UDM	411
GetPolicyAMF2PCF	412
UpdatePolicyAMF2PCF	413
GetPolicySMF2PCF	415
UpdatePolicySMF2PCF	416
RegistrationSMF2UDM	418
DeregistrationSMF2UDM	419
IntermediateSpendingLimitPCF2CHF	419

Primary Objective

Select **Primary Objective** from the UE Range pane to access the settings for the selected UE range's Primary Objectives.

The focus of the primary objectives is on the establishment of subscriber PDU sessions, wherein each session initiates one of the available procedures. The following Primary Objective types are available for configuration:

- **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.

Topics:

- [About primary objectives on the next page](#)
- [Active subscribers on page 398](#)
- [Subscribers per Second on page 403](#)

About primary objectives

In the current LoadCore 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 below](#)
- [Subscribers Per Second on the facing page](#)

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
Sustain time	Traffic and/or secondary objectives are executed
Ramp down	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.

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>	$2000 / 1000 = 20\text{s}$ for subscribers to deregister
<i>Rate in ramp down time:</i>	1000 deregistrations per second

Subscribers Per Second

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

Such a test will give the following results.

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

Active subscribers

When **Active Subscribers** is selected as the Primary Objective, 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. Each session will initiate the procedure that you select and configure.

- [Parameter Descriptions below](#)
- [UE Authentication Request AMF to AUSF below](#)
- [Create Policy AMF to PCF on the facing page](#)
- [Create Policy SMF to PCF on the facing page](#)
- [Initial Spending Limit PCF to CHF](#)
- [QoS Settings on page 401](#)
- [User Location on page 401](#)

Parameter Descriptions

The following table describes the configuration settings for the **Active Subscribers** objective.

Parameter	Description
Procedure Type	Select the procedure that will be started for this objective: <ul style="list-style-type: none"> • UE Authentication Request AMF to AUSF below • Create Policy AMF to PCF on the facing page • Create Policy SMF to PCF on the facing page • Initial Spending Control PCF to CHF
Ramp-up Rate	The number of subscriber sessions to activate per second.
Sustain Time (s)	The duration of time (in Seconds) that the specified sessions will remain 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.

UE Authentication Request AMF to AUSF

The the **UE Authentication Request AMF to AUSF** Procedure has a single configuration setting: *Starting AMF*. It takes one of the following values:

- **Start From First** - Starts from the first AMF in the list.
- **Start Round Robin** - First UE gets the first AMF, second UE the second AMF and so on.
- **Start Random** - Each UE gets a random AMF from the list.

Create Policy AMF to PCF

The following table describes the settings for the **Create Policy AMF to PCF** Procedure.

Procedure setting	Description
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
Access Type	Select the Access Network type for the policy: 3GPP Access or Non-3GPP Access.
RAT Type	Select the RAT type value to use for this policy association. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual. The RAT Type attribute indicates where the served UE is camping.

Create Policy SMF to PCF

The following table describes the settings for the **Create Policy SMF to PCF** Procedure.

Procedure setting	Description
PDU Session ID	Unsigned integer identifying a PDU session, within the range 0 to 255, as specified in clause 11.2.3.1b, bits 1 to 8, of 3GPP TS 24.007 [13].
PDU Type	Select the desired policy PDU type: IPv4 IPv6, IPv4, IPv6, UNSTRUCTURED, or ERHERNET.
DNN	Select one of the configured DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .
UE Time Zone	Specify the time zone value for this policy association. The time zone attribute (timeZone) indicates where the served UE is camping. The Time Zone information is expressed as the GMT time plus an offset value. The offset represents the time zone adjusted for daylight saving time.
Serving Network MCC	The MCC of the serving PLMN where the served UE is camping.
Serving Network MNC	The MNC of the serving PLMN where the served UE is camping.
Access Type	Select the Access Network type for the policy: 3GPP Access or Non-3GPP Access.
RAT Type	Select the RAT type value to use for this policy association. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual. The RAT Type attribute indicates where the served UE is camping.
Online	Select this option if the policy will support the online charging method for PDUs

Procedure setting	Description
	sessions.
Offline	Select this option if the policy will support the offline charging method for PDUs sessions.
Slice Info SD	Specify the Slice Differentiator (SD) value for the S-NSSAI associated with this policy. This is the S-NSSAI corresponding to the network slice that is allocated to the PDU (within the sliceInfo attribute).
Subs Session AMBR Uplink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Subs Session AMBR Downlink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink rate.
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
QoS Settings	Select <i>QoS Settings</i> to open the configuration panel for these settings, which are describe below in QoS Settings .
User Location	Select <i>NR Location</i> to open the configuration panel for these settings, which are describe below in User Location .

Spending Limit Control PCF to CHF

Parameter	Description
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
<i>Policy Counters</i>	
Policy Counters Ids	This parameter is used to identify a policy counter. Select a value from the drop-down list.
<i>Additional Policy Counters Ids</i>	
	Select this button to add additional policy counters ids.
	Select this button to remove the policy counter id.

QoS Settings

The Create Policy SMF to PCF procedure require QoS values for this objective's Service Data Flows. These configuration settings are described in the following table.

Parameter	Description
5QI	<p>Specify the 5QI value (decimal number) to use for this procedure.</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>
ARP:	
ARP Priority Level	<p>Specify the ARP priority level to use for this procedure.</p> <p>The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.</p>
ARP Preemption Capability	<p>Select Not Preemp or May Preempt.</p> <p>When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.</p>
ARP Preemption Vulnerability	<p>Select Not Preemptable or Preemptable.</p> <p>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.</p>

User Location

The User Location values are required by the services that enable an NF to request location information for a target UE. The User Location information includes:

- NR Location: The NR Location values are used in the 5G System by services that track the location of UEs.
- TAI: A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).
- NCGI: In the 5G System, each NR cell is assigned a NR Cell Global Identity (NCGI) value. It is formed by concatenating the PLMN-Id (PLMN Identifier) with the 36-bit NCI (NR Cell Identity).

These configuration settings are described in the following table.

Parameter	Description
<i>NR Location:</i>	
Age of Location information	The Age of Location Information value, at the start of the procedure. The value represents the elapsed time in minutes since the last network contact of the mobile station.
Geographical information	The Geographical Location value that the procedure will use in the identification of the UE location.
Geodetic information	The Geodetic Location value that the procedure will use in the identification of the UE location.
<i>TAI:</i>	
MCC	The PLMN MCC that is used in the construction of this TAI.
MNC	The PLMN MNC that is used in the construction of this TAI.
TAC	The PLMN TAC that is used in the construction of this TAI.
<i>NCGI:</i>	
MCC	The PLMN MCC that is used in the construction of this NCGI.
MNC	The PLMN MNC that is used in the construction of this NCGI.
NR Cell ID	The NCI that is used in the construction of this NCGI.

Subscribers per Second

When **Subscribers Per Second** is selected as the Primary Objective, the test attempts to activate a specified number of subscriber sessions per second, within the rate and time parameters that you configure. Each session will initiate the procedure that you select and configure.

- [Parameter Descriptions below](#)
- [UE Authentication Request AMF to AUSF below](#)
- [Create Policy AMF to PCF on the next page](#)
- [Create Policy SMF to PCF on the next page](#)
- [Initial Spending Limit PCF to CHF](#)
- [QoS Settings on page 406](#)
- [User Location on page 406](#)

Parameter Descriptions

The following table describes the configuration settings for the **Subscribers Per Second** objective.

Parameter	Description
Hold Time	The number of milliseconds 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.
Procedure Type	Select the procedure that will be started for this objective: <ul style="list-style-type: none"> • UE Authentication Request AMF to AUSF below • Create Policy AMF to PCF on the next page • Create Policy SMF to PCF on the next page • Initial Spending Limit PCF to CHF

UE Authentication Request AMF to AUSF

The the **UE Authentication Request AMF to AUSF** Procedure has a single configuration setting: *Starting AMF*. It takes one of the following values:

- **Start From First** - Starts from the first AMF in the list.
- **Start Round Robin** - First UE gets the first AMF, second UE the second AMF and so on.

- **Start Random** - Each UE gets a random AMF from the list.

Create Policy AMF to PCF

The following table describes the settings for the **Create Policy AMF to PCF** Procedure.

Procedure setting	Description
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
Access Type	Select the Access Network type for the policy: 3GPP Access or Non-3GPP Access.
RAT Type	Select the RAT type value to use for this policy association. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual. The RAT Type attribute indicates where the served UE is camping.

Create Policy SMF to PCF

The following table describes the settings for the **Create Policy SMF to PCF** Procedure.

Procedure setting	Description
PDU Session ID	Unsigned integer identifying a PDU session, within the range 0 to 255, as specified in clause 11.2.3.1b, bits 1 to 8, of 3GPP TS 24.007 [13].
PDU Type	Select the desired policy PDU type: IPv4 IPv6, IPv4, IPv6, UNSTRUCTURED, or ERHERNET.
DNN	Select one of the configured DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings on page 86 .
UE Time Zone	Specify the time zone value for this policy association. The time zone attribute (timeZone) indicates where the served UE is camping. The Time Zone information is expressed as the GMT time plus an offset value. The offset represents the time zone adjusted for daylight saving time.
Serving Network MCC	The MCC of the serving PLMN where the served UE is camping.
Serving Network MNC	The MNC of the serving PLMN where the served UE is camping.
Access Type	Select the Access Network type for the policy: 3GPP Access or Non-3GPP Access.
RAT Type	Select the RAT type value to use for this policy association. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual. The RAT Type attribute indicates where the served UE is camping.

Procedure setting	Description
Online	Select this option if the policy will support the online charging method for PDUs sessions.
Offline	Select this option if the policy will support the offline charging method for PDUs sessions.
Slice Info SD	Specify the Slice Differentiator (SD) value for the S-NSSAI associated with this policy. This is the S-NSSAI corresponding to the network slice that is allocated to the PDU (within the sliceInfo attribute).
Subs Session AMBR Uplink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Subs Session AMBR Downlink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink rate.
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
QoS Settings	Select QoS Settings to open the configuration panel for these settings, which are describe below in QoS Settings .
User Location	Select <i>NR Location</i> to open the configuration panel for these settings, which are describe below in User Location .

Spending Limit PCF to CHF

Parameter	Description
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
<i>Policy Counters</i>	
Policy Counters Ids	This parameter is used to identify a policy counter. Select a value from the drop-down list.
<i>Additional Policy Counters Ids</i>	
	Select this button to add additional policy counters ids.
	Select this button to remove the policy counter id.

QoS Settings

The Create Policy SMF to PCF procedure require QoS values for this objective's Service Data Flows. These configuration settings are described in the following table.

Parameter	Description
5QI	<p>Specify the 5QI value (decimal number) to use for this procedure.</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>
ARP:	
ARP Priority Level	<p>Specify the ARP priority level to use for this procedure.</p> <p>The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.</p>
ARP Preemption Capability	<p>Select Not Preemp or May Preempt.</p> <p>When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.</p>
ARP Preemption Vulnerability	<p>Select Not Preemptable or Preemptable.</p> <p>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.</p>

User Location

The User Location values are required by the services that enable an NF to request location information for a target UE. The User Location information includes:

- NR Location: The NR Location values are used in the 5G System by services that track the location of UEs.
- TAI: A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).
- NCGI: In the 5G System, each NR cell is assigned a NR Cell Global Identity (NCGI) value. It is formed by concatenating the PLMN-Id (PLMN Identifier) with the 36-bit NCI (NR Cell Identity).

These configuration settings are described in the following table.

Parameter	Description
<i>NR Location:</i>	
Age of Location information	The Age of Location Information value, at the start of the procedure. The value represents the elapsed time in minutes since the last network contact of the mobile station.
Geographical information	The Geographical Location value that the procedure will use in the identification of the UE location.
Geodetic information	The Geodetic Location value that the procedure will use in the identification of the UE location.
<i>TAI:</i>	
MCC	The PLMN MCC that is used in the construction of this TAI.
MNC	The PLMN MNC that is used in the construction of this TAI.
TAC	The PLMN TAC that is used in the construction of this TAI.
<i>NCGI:</i>	
MCC	The PLMN MCC that is used in the construction of this NCGI.
MNC	The PLMN MNC that is used in the construction of this NCGI.
NR Cell ID	The NCI that is used in the construction of this NCGI.

Secondary Objectives

For each primary objective that you define, you can add one or more Secondary Objectives for the selected UE range.

When you select **Secondary Objective** from the UE **Range** pane, LoadCore opens another panel in which you can add one or more Secondary Objectives. These objectives are associated to the single Primary Objective configured for the UE range.

To add a Secondary Objective:

1. Click the **Add** button in the Objectives pane.



LoadCore opens the **Settings** pane where you configure the new objective.

2. In the new objective's **Settings** pane, select the desired *Procedure* from the drop-down list.
(LoadCore automatically selects the first Procedure from the list.)
3. Configure all of the procedures for the new objective.

Topics:

UEGetNSSAIAMF2UDM	409
RegistrationAMF2UDM	410
DeregistrationAMF2UDM	411
GetPolicyAMF2PCF	412
UpdatePolicyAMF2PCF	413
GetPolicySMF2PCF	415
UpdatePolicySMF2PCF	416
RegistrationSMF2UDM	418
DeregistrationSMF2UDM	419
IntermediateSpendingLimitPCF2CHF	419

UEGetNSSAIAMF2UDM

The following table describes the **Settings** for the *UEGetNSSAIAMF2UDM* Secondary Objective. This objective executes a procedure in which the AMF (the NF service consumer) sends a request to the UDM to obtain the UE's subscribed NSSAI.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	UE Get NSSAI AMF to UDM.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>UE Get NSSAI AMF to UDM:</i>	
Include Supported Features	Select this option if the procedure will include "supported-features" in the query.
Supported Features Query	Enter the supported-features value to use for the query.
Include PLMN ID	Select this option if the procedure will include "plmn-id" in the query.
PLMN ID Query	Enter the PLMN ID value to use for the query.

RegistrationAMF2UDM

The following table describes the **Settings** for the *RegistrationAMF2UDM* Secondary Objective. This objective executes a procedure in which the AMF that is providing service to the UE invokes the Registration service operation to store related UE Context Management information in the UDM.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Registration AMF to UDM.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>Registration AMF to UDM:</i>	
Role	Select the role for this procedure: <ul style="list-style-type: none"> • Initial Registration – executes only when there is no AMF currently registered for the UE (either at start or when deregistered). • Inter AMF Mobility – executes after initial registration and does inter-AMF mobility registration • Initial And Mobility – does both the initial and the mobility AMF registration.
Next AMF	Describes how the next AMF is selected when doing AMF mobility registration: <ul style="list-style-type: none"> • Next Round Robin – selects the next AMF from the list in round-robin fashion. • Next Random – selects the next AMF from the list randomly.

DeregistrationAMF2UDM

The following table describes the **Settings** for the *DeregistrationAMF2UDM* Secondary Objective. This objective executes a procedure in which the AMF sends a request to the UDM to deregister a UE.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Deregistration AMF to UDM.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>Deregistration AMF to UDM:</i>	
Min Hold Time (ms)	Minimum time (ms) that must elapse between an AMF registration procedure and this deregistration procedure.

GetPolicyAMF2PCF

The following table describes the **Settings** for the *GetPolicyAMF2PCF* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Get Policy AMF to PCF.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.

UpdatePolicyAMF2PCF

The following table describes the **Settings** for the *UpdatePolicyAMF2PCF* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Update Policy AMF to PCF.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>User Location:</i>	
NR Location	Select NR Location to open the configuration panel for the User Location settings (described below).

User Location

The User Location values are required by the services that enable an NF to request location information for a target UE. The User Location information includes:

- NR Location: The NR Location values are used in the 5G System by services that track the location of UEs.
- TAI: A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).
- NCGI: In the 5G System, each NR cell is assigned a NR Cell Global Identity (NCGI) value. It is formed by concatenating the PLMN-Id (PLMN Identifier) with the 36-bit NCI (NR Cell Identity).

These configuration settings are described in the following table.

Parameter	Description
<i>NR Location:</i>	
Age of Location information	The Age of Location Information value, at the start of the procedure. The value represents the elapsed time in minutes since the last network contact of the mobile station.

Parameter	Description
Geographical information	The Geographical Location value that the procedure will use in the identification of the UE location.
Geodetic information	The Geodetic Location value that the procedure will use in the identification of the UE location.
<i>TAI:</i>	
MCC	The PLMN MCC that is used in the construction of this TAI.
MNC	The PLMN MNC that is used in the construction of this TAI.
TAC	The PLMN TAC that is used in the construction of this TAI.
<i>NCGI:</i>	
MCC	The PLMN MCC that is used in the construction of this NCGI.
MNC	The PLMN MNC that is used in the construction of this NCGI.
NR Cell ID	The NCI that is used in the construction of this NCGI.

GetPolicySMF2PCF

The following table describes the **Settings** for the *GetPolicySMF2PCF* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Get Policy SMF to PCF.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.

UpdatePolicySMF2PCF

The following table describes the **Settings** for the *UpdatePolicySMF2PCF* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Update Policy SMF to PCF.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>Update Policy SMF to PCF:</i>	
Policy Control Request Triggers	<p>The policy control request triggers which are met.</p> <p>Possible values are:</p> <ul style="list-style-type: none"> • PLMN_CH – PLMN Change • RES_MO_RE – a request for resource modification has been received by the SMF. The SMF always reports to the PCF. • AC_TY_CH – Access Type Change • UE_IP_CH – UE IP address change. The SMF always reports to the PCF. • UE_MAC_CH – a new UE MAC address is detected or a used UE MAC address is inactive for a specific period • AN_CH_COR – Access Network Charging Correlation Information • US_RE – the PDU Session or the Monitoring key specific resources consumed by a UE either reached the threshold or needs to be reported for other reasons. • APP_STA – the start of application traffic has been detected. • APP_STO – the stop of application traffic has been detected. • AN_INFO – Access Network Information report • CM_SES_FAIL – credit management session failure • PS_DA_OFF – the SMF reports when the 3GPP PS Data Off status changes. The SMF always reports to the PCF.

Parameter	Description
	<ul style="list-style-type: none"> • DEF_QOS_CH – default QoS Change. The SMF always reports to the PCF. • SE_AMBR_CH – session AMBR Change. The SMF always reports to the PCF. • QOS_NOTIF – the SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be guaranteed or guaranteed again. • NO_CREDIT – Out of credit • PRA_CH – change of UE presence in Presence Reporting Area • SAREA_CH – Location Change with respect to the Serving Area • SCNN_CH – Location Change with respect to the Serving CN node • RE_TIMEOUT – indicates the SMF generated the request because there has been a PCC revalidation timeout • RES_RELEASE – indicates that the SMF can inform the PCF of the outcome of the release of resources for those rules that require so. • SUCC_RES_ALLO – indicates that the requested rule data is the successful resource allocation. • RAT_TY_CH – RAT Type Change. • REF_QOS_IND_CH – Reflective QoS indication Change
Number of Packet Filters	Specify the number of supported packet filters for signaled QoS rules.
3GPP Ps Data Off Status	If it is included in selected, the 3GPP PS Data Off is activated by the UE.
QoS Flow Usage	<p>Available options:</p> <ul style="list-style-type: none"> • GENERAL – indicates that no specific QoS flow usage information is available. • IMS_SIG – indicate that the QoS flow is used for IMS signaling only.
RES_MO_RE Data json	The JSON of the ueInitResReq IE from Npcf SM Policy Control Update request. The JSON represents the request for resource modification.

RegistrationSMF2UDM

The following table describes the **Settings** for the *RegistrationSMF2UDM* Secondary Objective. This objective executes a procedure in which the SMF sends a request to the UDM to create a new registration.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Registration SMF to UDM.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>Registration SMF to UDM:</i>	
SMF ID	The SMF ID of the SMF to which the request will be sent.
SNSSAI SST	The SST (Slice/Service Type) value for the NSSAI that will be used for the requested registration. SST comprises octet 3 in the NSSAI information element.
SNSSAI SD	The SD (Slice Differentiator) value for the NSSAI that will be used for the requested registration. SD comprises octets 4 through 6 in the NSSAI information element.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .

DeregistrationSMF2UDM

The following table describes the **Settings** for the *DeregistrationSMF2UDM* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Deregistration SMF to UDM.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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.
Trigger	Select the manner in which the objective is triggered: Manual or Automatic (default value). When the trigger objective is set to Automatic , the secondary objectives will start automatically. When it is set to Manual , the secondary objective will start only if it receives the <code>start</code> command.
Delay (s)	The number of seconds that will elapse before the start of the procedure.
<i>Deregistration SMF to UDM:</i>	
Min Hold Time (ms)	Minimum time (ms) to pass between a SM FRegistration procedure and this procedure (deregistration).

IntermediateSpendingLimitPCF2CHF

The following table describes the **Settings** for the *IntermediateSpendingLimitPCF2CHF* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Intermediate Spending Limit PCF to CHF.
Only Once	When this option is selected, the test performs a single iteration of the procedure. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.

Parameter	Description
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 that will elapse before the start of the procedure.
<i>Intermediate Spending Limit PCF to CHF</i>	
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).

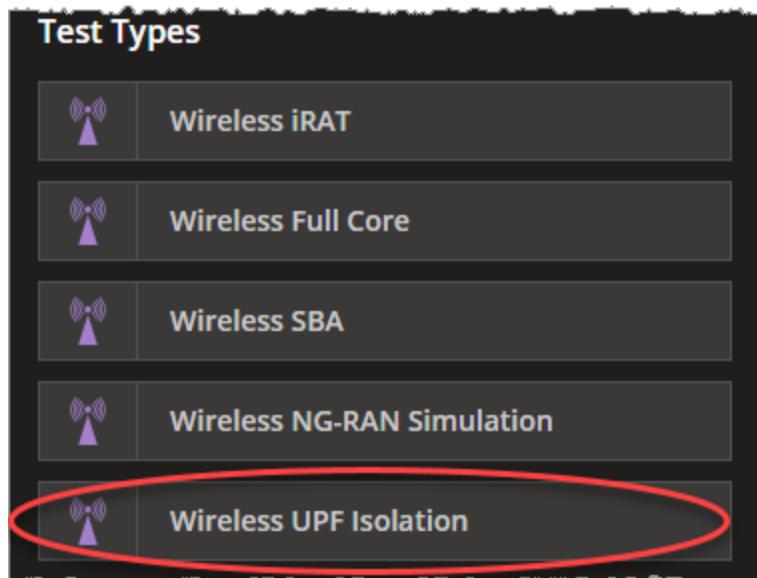
The following table describes the Intermediate Policy Counters settings.

Parameter	Description
<i>Intermediate Policy Counters Ids</i>	
Policy Counters Ids	This parameter is used to identify a policy counter. Select a value from the drop-down list.
<i>Additional Policy Counters Ids</i>	
	Select this button to add additional policy counters ids.
	Select this button to remove the policy counter id.

CHAPTER 9

UPF Isolation tests: configuration settings

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



In an UPF Isolation test topology, the DUT is UPF and LoadCore simulates traffic on the N3, N4, and N6 interfaces. You configure the simulated UEs, NG-RAN, SMF, and DN as required by your test requirements.

Topics:

Global Settings panel	424
DNS Settings	425
Advanced Settings	425
Impairment	428
QoS Flows panel	429
QoS Flow configuration settings	429
Reporting Settings	431
UE configuration settings	432
UE Ranges panel	433

UE Range panel	434
UE range settings	435
Objectives	440
Control Plane Objective	440
About primary objectives	441
Primary Control Plane Objective	443
Secondary Control Plane Objectives	445
User Plane Objectives	453
Stateless UDP Traffic Generator	455
Data Traffic	456
Voice Traffic	458
DNS Client Traffic	461
Video OTT Traffic	464
Predefined Applications Traffic	467
SMF configuration settings	478
SMF Ranges panel	479
SMF Range settings	479
SMF N4 interface settings	480
SMF Uplink Paths	482
RAN configuration settings	483
RAN Ranges panel	484
RAN Range settings	484
RAN N3 interface settings	485
Passthrough interface settings	486
UPF configuration settings	487
UPF Ranges panel	488
UPF Range panel	488
UPF N3 interface settings	489
UPF N4 interface settings	490
UPF N6 interface settings	492
UPF N9 interface settings	493
UPF N4u interface settings	494

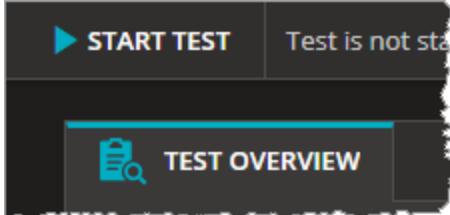
DN configuration settings	497
DN Ranges panel	497
DN Range panel	497
DN N6 Interface settings	498
DN UE routes settings	499
DN User Plane	500
DN Application Traffic Generator	500
DN Stateless UDP Traffic Generator	507

Global Settings panel

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:

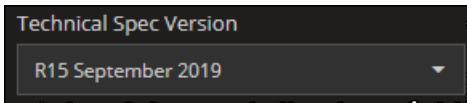


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



LoadCore 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:

DNS Settings **425**

Advanced Settings **425**

Impairment **428**

QoS Flows panel **429**

 QoS Flow configuration settings 429

 Reporting Settings 431

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 miliseconds) 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 and the ones needed for GTPU tunnel traffic.

Setting	Description
Overwrite Capture Size for IxStack	Select this check box 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 check box to enable it.
Enable Capture On Loopback Interface	Select this check box to enable packet capture on the loopback interface.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: <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.

Setting	Description
	<ul style="list-style-type: none"> • Delay Variation Jitter - the per polling interval average delay variation jitter value calculated for all packets.
Enable Control Plane Advanced Stats	<p>Select this check-box to enable control plane latency statistics.</p>
Use NIC MAC address for all protocol interfaces on RAN, UPF, and DN	<p>This option is available to support SRIOV (Single-Root I/O Virtualization) test setups. With SRIOV, only the virtual function's MAC address can be used for protocol interfaces.</p> <p>When this option is enabled:</p> <ul style="list-style-type: none"> • All IP addresses from all the network interfaces that are mapped on the ixstack interface will be configured on the test interface with the virtual function's MAC address. • The virtual function's MAC address is automatically inserted by LoadCore (it will override the MAC address that is configured in the web interface). <p>When option is disabled, LoadCore will use the MAC address defined in the web interface for each IP address definition.</p>
Automated Polling Interval	<p>Selected by default. The statistics are retrieved based on a predefined polling interval.</p>
Custom Polling Interval (sec)	<p>This option becomes available only when Automated Polling Interval check-box is unselected.</p> <p>It allows you to create a custom polling interval.</p>
Log Level	<p>Select one of the options:</p> <ul style="list-style-type: none"> • Info - Designates informational messages that highlight the progress of the application at coarse-grained level. • Debug - Designates fine-grained informational events that are most useful to debug the application.
Log Tags	<p>Select one or more tags from the drop-down list.</p> <p>Log Tags are used to collect specific information in the logs; they work with Debug and with Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.</p>
Ignore Offline Agents At Runtime	<p>When this option is selected, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.</p>

The following table describes the settings required 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	DESCRIPTION IS NOT YET AVAILABLE.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select the check box to enable this option.
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.

Control Plane Latency Statistics

For the Control Plane Latency Statistics, the latency is measured per procedure. The latency statistics are available only for PFCP.

The control plane procedure latency value represents the time between the moment when the first message in the procedure is sent or received and the moment when the last message in the procedure is sent or received.

IMPORTANT The time shown in statistics may be slightly different than the time computed in any capturing tool (for example, Wireshark) because of the time when the packets are actually captured.

Latency buckets:

- 0us - 125us
- 125us - 250us
- 250us - 500us
- 500us - 1ms
- 1ms - 5ms
- 5ms - 10ms
- 10ms - 15ms
- 15ms - 20ms
- 20ms - inf

NOTE If enabled, the control plane latency statistics will not be displayed in predefined dashboards in LoadCore statistics user interface. To display these statistics you will need to use custom dashboards.

Retrieve captured packets

After enabling packet capture, and running the test, to download the generated packet captures, you need to use a SFTP client (for example, WinSCP) to retrieve the captures from `/opt/5gc-test-engine` on each of the agents.

The packet capture can be identified as follows:

- `latestCapture.pcap`, when running the test without DPDK activated
- `latestIxStackCapture.pcap` when running the test with DPDK activated

Impairment

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

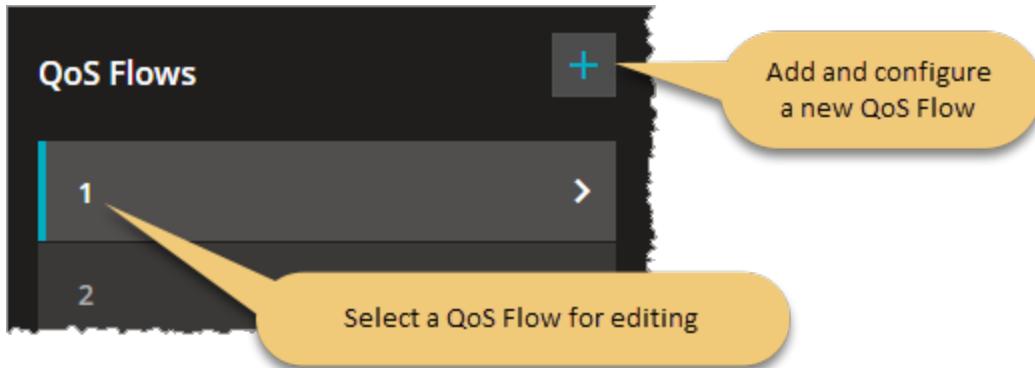
Setting	Description
<i>Impairment Profiles:</i>	
 +	Select the Add impairment profile button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the Delete impairment profile button to remove the profile from your test configuration.
Name	Each impairment profile is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Action Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Custom script • PFCP-drop message
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 5G QoS model is based on QoS Flows. A 5G QoS Flow is the finest level of granularity for QoS forwarding treatment in the 5G System. All traffic mapped to the same 5G QoS Flow receives the same forwarding treatment.

Accessing the configuration settings:

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



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

QoS Flow configuration settings **429**

Reporting Settings **431**

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 following table.

Setting	Description
Is Default	Select this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow. If this option is not selected, LoadCore displays the SDF settings (described below).
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

Setting	Description
	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.
Application ID	The Application ID set in PDI. This option will be present in the PDI (for each direction, UL and DL) of each flow for which the option was configured.

SDF settings

These Service Data Flow settings are available for any QoS Flow that is not selected as the default flow (the *Is Default* option is disabled). For these non-default flows, you need to configure the Maximum Bit Rate and Guaranteed Bit Rate values.

Setting	Description
SDF string	<p>Enter an SDF string that describes the packet filter. For example:</p> <pre>permit out 17 from 22.22.22.22 11111 to \$ueip\$ 11100</pre> <p>In this example:</p> <ul style="list-style-type: none"> • the Action is 'permit' • the Direction is 'out' • the Protocol Number is 17 (UDP) • the Source IP address is 22.22.22.22 • the Source Port is 11111 • The Destination IP is <i>\$ueip\$</i> (a format specifier for UE IP address) • The Destination Port is 11100. <p>The SDF String option is available for any QoS flow, including the default flow (s).</p> <p>The SDF syntax details are described in TS 29.212, section 5.4.2.</p>
<i>MBR</i>	
Uplink (kbps)	The MBR uplink bitrate.
Downlink (kbps)	The MBR downlink bitrate.
<i>GBR</i>	
Uplink (kbps)	The GBR uplink bitrate.
Downlink (kbps)	The GBR downlink bitrate.

Activate predefined rules

This option is used to add a predefined rule on a per flow basis.

NOTE

For backwards compatibility, rules can still be activated on a per UE Range basis ([Activate Predefined Rules](#)). If rules are configured on both UE range and QoS Flow, the QoS Flow settings will take precedence.

The **Active Predefined Rules** settings are described in the following table.

<i>Active Predefined Rules:</i>	
	Select the Add Activate Predefined Rules button to add a predefined rule to your test configuration.
	Select the Delete button to remove the redefined rule from your test configuration.

Reporting Settings

The values that you configure in the QoS Flows **Reporting Settings** populate the Volume Threshold and Volume Quota information elements (IEs) for the selected QoS Flow.

The Volume Threshold and/or Volume Quota IEs may be present in the Create URR grouped IE. Usage Reporting Rules (URRs) contain instructions for creating traffic measurement and reporting. The Volume Threshold IE is included if reporting is required upon reaching a volume threshold. The Volume Quota IE is included if volume-based measurement is used and the CP function needs to provision a Volume Quota in the UP function. Reference: 3GPP TS 29.244.

Setting	Description
<i>Volume Threshold</i>	
Total	The number of octets for the Total Volume field of the Volume Threshold IE.
Uplink	The number of octets for the Uplink Volume field of the Volume Threshold IE.
Downlink	The number of octets for the Downlink Volume field of the Volume Threshold IE.
<i>Volume Quota</i>	
Total	The number of octets for the Total Volume field of the Volume Quota IE.
Uplink	The number of octets for the Uplink Volume field of the Volume Quota IE.
Downlink	The number of octets for the Downlink Volume field of the Volume Quota IE.

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:

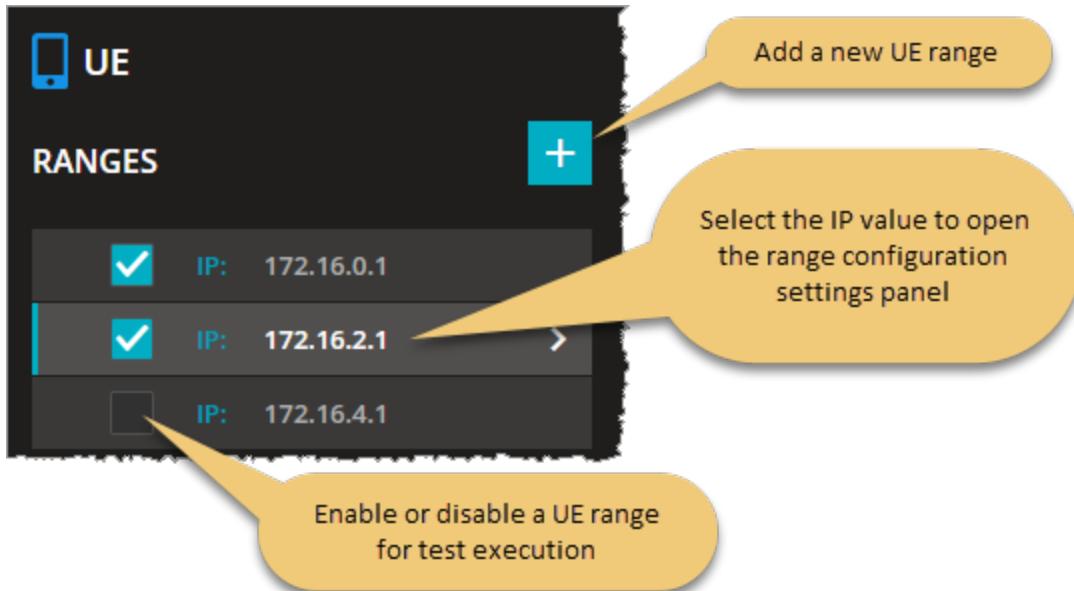
UE Ranges panel	433
UE Range panel	434
UE range settings	435

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 ...



Refer to [UE Range panel on the next page](#) for a description of the UE range settings.

UE Range panel

When you select an IP address from the UE **Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- Delete the UE range from the test configuration.
- Configure the *Range Count*.
- Select the *Parent NG-RAN*, *Parent SMF* and *Uplink Path* for the UE range.
- Access the detailed UE configuration settings (Identification, Settings, QoS Config).
- Access the Objectives settings for the range.

UE range controls and settings

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

Setting	Description
<i>Basic range settings:</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 NG-RAN	Select the desired NG-RAN from the test configuration. This will be the NG-RAN through which the UEs in the range will access the 5G core network.
Parent SMF	Select the desired parent SMF from the drop-down list.
Uplink Path	Select the uplink path from the drop-down list.
<i>Detailed range settings:</i>	
Identification	Refer to the following topic for descriptions of the UE Identification settings: Identification settings on the facing page .
Settings	Refer to the following topic for descriptions of the UE Settings settings: Settings settings on page 436 .
QoS Config	Refer to the following topic for descriptions of the UE QoS Config settings: QoS Config settings on page 439 .

Objectives

Each UE range has its own objectives settings. Refer to [Objectives on page 440](#) for detailed descriptions.

UE range settings

For each range that you add to your test configuration, you configure the settings described in the **Range** panel ([UE Range panel on page 244](#)), plus the settings described below.

Identification settings

The following table describes the UE Identification settings.

Setting	Description
PDU Type	Select the type of PDU for this session: <ul style="list-style-type: none"> IP Ethernet
IP Type	Select the type of IP address used in test: <ul style="list-style-type: none"> IPv4 IPv6 IPv4V6
<i>Ipv4</i>	<i>This option is available only when IP Type is set to IPv4.</i>
Ipv4	The IPv4 address that has been assigned to your UE range.
IPv4 Increment	The value to use for incrementing the IPv4 addresses of your UE range.
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.
<i>Ipv6</i>	<i>This option is available only when IP Type is set to IPv6.</i>
Ipv6	The IPv6 address that has been assigned to your UE range.
IPv6 Increment	The value to use for incrementing the IPv6 addresses of your UE range.
IPv6 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>Ipv4V6</i>	<i>This option is available only when IP Type is set to IPv4V6. This allows you to configure both the IPv4 stack and the IPv6 stack.</i>
Ipv4	The IPv4 address that has been assigned to your UE range.
IPv4 Increment	The value to use for incrementing the IPv4 addresses of your UE range.
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.

Setting	Description
Ipv6	The IPv6 address that has been assigned to your UE range.
IPv6 Increment	The value to use for incrementing the IPv6 addresses of your UE range.
IPv6 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.
Include IMSI in UserID IE	Select this check box to include the IMSI in the UserID IE.
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.
Include MSISDN in UserID IE	Select this check box to include the MSISDN in the UserID IE.
MSISDN	The first Mobile Station ISDN (MSISDN) value for this range.
MSISDN Increment	The value to use for incrementing the MSISDNs in the range.
Include IMEISV in UserID IE	Select this check box to include the IMEI SV in the UserID IE.
IMEI SV	The IMEI SV value that will be assigned to the first simulated UE in the range.
IMEI SV Increment	The value to use for incrementing the IMEISV values for each of the UEs in the range.
Ethernet Device Information	Allows adding multiple ethernet devices per DNN with PDU type Ethernet.
Ethernet PDU config	For each ethernet device the MAC Address, IP Address, outer VLAN and inner VLAN can be configured.

Settings settings

The following table describes the UE Settings settings.

Setting	Description
<i>Settings:</i>	
Bidirectional SDF Filters	Enable this option to set the BID (Bidirectional SDF Filter) flag to 1 in the SDF Filter IE. This flag is bit 5 in octet 5. When this flag is set, the SDF Filter ID will be present in the IE. Bidirectional SDF Filters are associated to both uplink and downlink Packet Detection Rules (PDRs) of the same Sx session.
Enable Passthrough	Select this option to enable passthrough. When passthrough is enabled, on the passthrough interface, the LoadCore waits for packets. Once received, the packets are encapsulated and transferred via N3 to the other side of the network.
Enable SLAAC	This option enables IPv6 UEs to get their IP addresses via SLAAC (Stateless Address Auto-configuration). <p>NOTE The UE configured IPs must be IPv6. The User Plane uplink/downlink objectives server IP (destination for uplink, source for downlink) should also be IPv6.</p> <p>If SLAAC is enabled on an UE range, during the Session Establishment procedure, the SMF and UPF negotiate a N4-u tunnel (distinct from N4). A SLAAC configured UE sends (via gNB) a Router Solicitation message on N3 towards the UPF. The UPF forwards the Router Solicitation towards the SMF on the N4-u interface. The SMF replies with a Router Advertisement on N4-u towards the UPF, then the UPF forwards it back to the gNB on N3. The Router Advertisement contains the IPv6 prefix the UE will use in the subsequent traffic.</p>
Network Instance Format	Select the encoding format for the network instance: string or label-list.
N3 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.
N4-u Network Instance	It represents the value to be sent in the Network Instance IE when the source interface is set N4-u. This value will be used to locally configure a N4-u network instance, overwriting the one advertised by the UPF (if any).
N6 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.
<i>BAR Settings: These settings are used in the Update BAR procedure for idle UEs.</i>	
Delay Before Update BAR	The delay in milliseconds before the UE will send a Session Modification Request with an UpdateBAR IE. This can occur while the UE is in idle (it happens only one time).
Downlink Data Notification Delay	The delay that the UP will apply between receiving a downlink data packet and notifying the CP function about it. Delay Value in integer multiples of 50 milliseconds, or 0 (TS 29244 8.2.28).

Setting	Description
Suggested Buffering Packets Count	The count of suggested buffering packets.
<i>Data Network Name:</i>	
Data Network Name	<p>Set the Data Network Name(DNN) value. For example: <code>myHome.com</code>. An empty value is accepted as input for this parameter.</p> <p>When a value is added it will be sent in PFCP Session Establishment Request message in APN IE.</p> <p>This value is the same for all UEs in range.</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> <p>NOTE The <code>start_value</code> and <code>end_value</code> must have the same length. For example, we can configure <code>dnn[008-999,1]</code> and obtain <code>dnn008,dnn009,...,dnn998,dnn999</code>. Syntaxes <code>dnn[8-999,1]</code> or <code>[008-1000,1]</code> are not valid as the start and end value lengths are different.</p> <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> <p>IMPORTANT If multiple sequence generators are configured and their pools overlap (for example: <code>dnn[000-600,1].keysight.com</code> <code>dnn[500-999,1].keysight.com</code>), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the <code>start_value</code> (they might start with an intermediate value in the second pool).</p>
<i>Active Predefined Rules:</i>	
	Select the Add Activate Predefined Rules button to add a predefined rule to your test configuration.

Setting	Description
	Select the Delete button to remove the redefined rule from your test configuration.

QoS Config settings

In the 5G system, QoS is enforced controlled at the QoS flow level. When you configure LoadCore UE ranges, you can associate each range with one or more QoS flows that you have configured in the Global settings, and you can choose to enable QoS detection and enforcement for each UE range.

The following table describes the UE QoS Config settings.

Setting	Description
<i>QoS Config:</i>	
Use Detective	Select the check-box to enable QoS flow level traffic detection for QoS enforcement. It monitors traffic and measures the data volume that surpasses the QoS limit.
Use Enforcement	Select the check-box to enable QoS enforcement. It blocks traffic when the data volume has reached the QoS limit.
Flows	Select one or more flows from the list of QoS flows.
<i>AMBR:</i>	
Uplink (kbps)	The uplink Session-AMBR value for this UE range.
Downlink (kbps)	The downlink Session-AMBR value for this UE range.

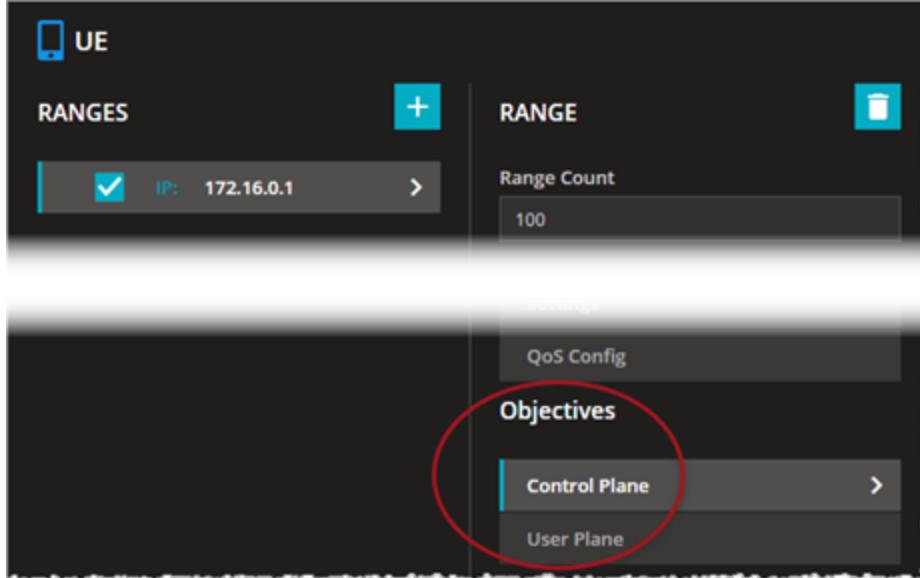
Objectives

In a LoadCore 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.

There are two categories of test objectives:

- [Control Plane Objective below](#)
- [User Plane Objectives on page 453](#)

The test Objectives are individually configured for each UE range. For example:



The Control Plane objectives always take precedence over User Plane objectives when running in parallel. This means that a test will first try to achieve the Control Plane objectives, and only then attempt to achieve the User Plane objective (Throughput, and so forth).

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:

- [Primary Control Plane Objective on page 443](#)
- [Secondary Control Plane Objectives on page 445](#)
- [About primary objectives on the facing page](#)

About primary objectives

In the current LoadCore 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 below](#)
- [Subscribers Per Second on the next page](#)

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
Sustain time	Traffic and/or secondary objectives are executed
Ramp down	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 (`<number_of_subscribers_in_the_range> / <RampUpRate>`). If the ramp up rate cannot be maintained, ramp up will last longer.
- During the sustain time phase, only secondary objectives are running.
- If configured, uplink traffic will start after the ramp up stage is complete.
- Subscribers will accept any downlink traffic once they are attached (registered and PDU session established).
- The duration of ramp down is not directly configurable. The ramp down time is automatically computed from the total number of subscriber in the range divided by the configured Ramp-up Rate (`<number_of_subscribers_in_the_range> / <RampUpRate>`). If the ramp down rate cannot be maintained, ramp down will last longer.

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>	$2000 / 1000 = 20\text{s}$ for subscribers to deregister
<i>Rate in ramp down time:</i>	1000 deregistrations per second

Subscribers Per Second

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

Such a test will give the following results.

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

Primary Control Plane Objective

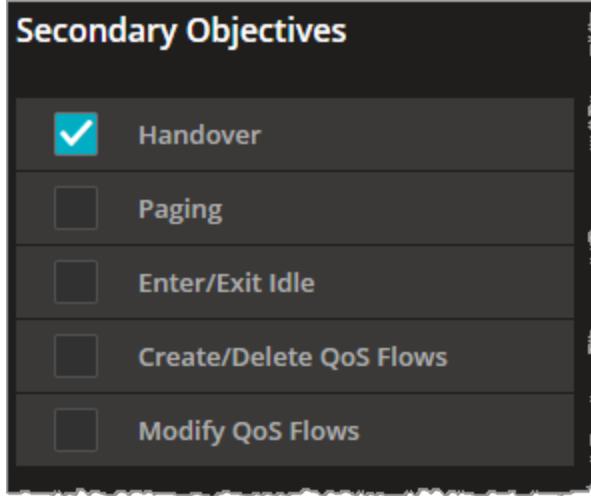
The following table describes the **Primary** control plane objectives.

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.
Flows to Activate	Select the list of QoS flow IDs to create during session establishment.
<i>Subscribers Per Second:</i>	
Hold Time	The number of milliseconds 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.

Parameter	Description
Delay (s)	The number of seconds to wait before starting the objective.
Flows to Activate	Select the list of QoS flow IDs to create during session establishment.

Secondary Control Plane Objectives

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. In this example, only Handover has been selected:



Note that:

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

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 on page 434](#)). The UEs then traverse the NG-RANs that you configure (the *Visited NG-RAN* list).

The following table describes these objective parameters.

Parameter	Description
<i>Handover:</i>	
Only Once	When this option is selected, the test performs a single iteration of the objective. Therefore, each UE moves through the entire mobility path, but only one time. When this option is not selected, the test executes handovers at the specified rate during the entire duration of the test. In this case, the UEs may move through the mobility path more than once.
Rate	The rate at which handovers are initiated, measured in handovers per second.
Max	The maximum number of Handover procedures that may be outstanding while

Parameter	Description
Outstanding	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 delay between each handover event in the handover path, in seconds.
<i>Visited GNBS</i>	
Visited NG-RAN	<p>A list of the NG-RANs that UEs will visit during the test. Use the following controls to manage the NG-RAN list:</p> <div style="display: flex; justify-content: space-between;">  Add next NG-RAN to the list  Remove the selected NG-RAN from the list </div>

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>	
Only Once	When this option is selected, the procedure is ran only once for each subscriber. When this option is not selected, the test executes the procedure at the specified rate throughout the entire duration of the test.
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
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 time (in seconds) to wait before starting the secondary objective, after sustain is reached.
Suspend Traffic Interval (s)	The time (in seconds) to suspend traffic on the remote IP address.
Remote IP	Set the remote IP address:

Parameter	Description
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.

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 the Enter/Exit Idle procedure is set and the UE has to exit Idle to perform a different procedure, the Enter/Exit Idle procedure is still scheduled to perform Exit Idle, but the UE is not in Idle anymore. In this case, 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.

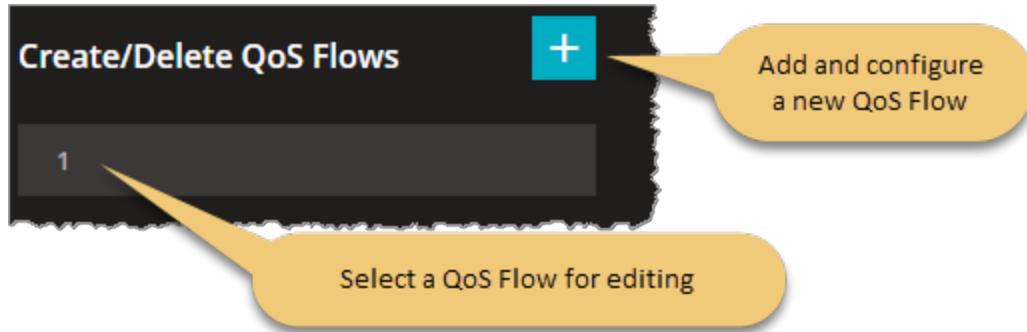
The following table describes the objective parameters.

Parameter	Description
<i>Enter Exit Idle:</i>	
Only Once	When this option is selected, the test performs a single iteration of the objective. Therefore, each UE enters and exits the CM-IDLE state, but only one time. When this option is not selected, the test executes enters and exits the CM-IDLE state at the specified rate during the entire duration of the test. In this case, the UEs may enter and exit the CM-IDLE state more than once.
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.
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 that will elapse before the start of the Idle transition event simulation.
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 create new QoS flows or delete existing QoS flows. The create/delete actions will be based on the configuration settings that you establish for this objective.

In the **Create/Delete QoS Flow** panel, you can add instances to your objective and select already-defined instances for modification or deletion:



The following table describes the Objective parameters.

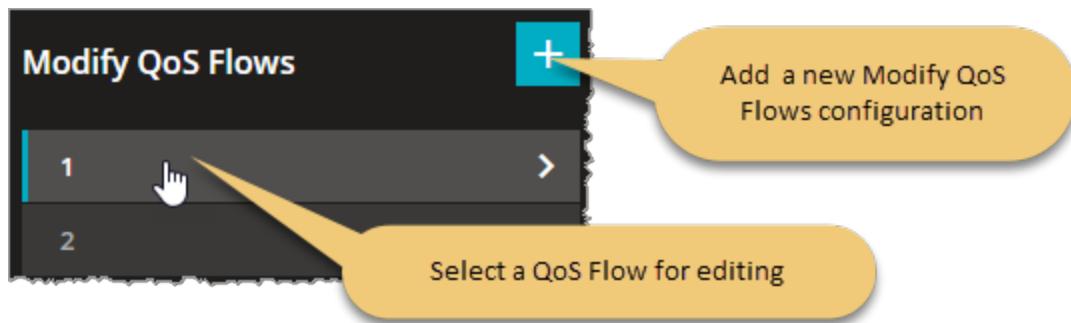
Parameter	Description
<i>Objective:</i>	
	Select the Delete Objective button to delete this QoS flow from your objective configuration.
Only Once	When this option is selected, the test performs a single iteration of the objective.
Rate	The rate at which procedures are initiated.
Max Outstanding	The maximum 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, once the sustain value is reached.
Interval	The number of seconds to wait between each successive action.
<i>Flow IDs: Select the Flows ID from the drop-down list.</i>	
	Add a new Flow ID to the list (internal identifier of the QoS Flow).
	Remove the selected Flow ID from the list

Modify QoS Flows

When you configure a **Modify QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to execute a UE-requested PDU Session Modification procedure. The procedure execution will be based on the configuration settings that you establish for this objective.

Known Issue! When running Modify QoS Flow objective for the default QoS flow and the *Only Once* parameter is set to False, all Session Modification Request messages for the same subscriber will be populated with the same values for the Update PDR parameters (Precedence / Activate Predefined Rules / Deactivate Predefined Rules).

In the **Modify QoS Flow** panel, you can add instances to your objective and select already-defined instances for modification or deletion:



The following table describes the Objective parameters.

Parameter	Description
<i>Objective:</i>	
	Select the Delete Objective button to delete this QoS flow from your objective configuration.
Only Once	When this option is selected, the test performs a single iteration of the objective.
Rate	The rate at which procedures are initiated.
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 that will elapse before the start of the action defined by the objective.
Trigger	In the LoadCore Web UI, the trigger is always automatic (that is, the secondary objectives will start automatically). In contrast, the REST API allows for a manual trigger.
Update PDR	These settings are described in Update PDR on the next page below.

Parameter	Description
Update QoS	These settings are described in Update QoS on the facing page below.
Update URR	These settings are described in Update URR on page 452 below.

Update PDR

To add an update for the packet detection rule (PDR) to your **Modify QoS Flow** configuration, select the **Add Update PDR** button.



The following table describes the parameters required to update the packet detection rule.

Parameter	Description
<i>Update PDR Settings:</i>	
	Select the Delete Update PDR button to delete this Update PDR from your objective configuration.
Flow ID	Select the flow ID from the drop-down list.
Direction	Select the traffic direction for which this filter applies: Uplink or Downlink.
Precedence	Specify the desired PDR Precedence value for this Update PDR. The the PDR precedence value determine the order in which a PDR will be evaluated. The evaluation of the PDRs is performed in increasing order of their precedence value.
<i>Activate Predefined Rules: List of predefined rules to be activated.</i>	
	Select the Add Activate Predefined Rules button to add a predefined rule to your test configuration.
	Select the Delete button to remove the redefined rule from your test configuration.
<i>Deactivate Predefined Rules: List of predefined rules to be deactivated.</i>	
	Select the Add Activate Predefined Rules button to deactivate a predefined rule to your test configuration.

Parameter	Description
	Select the Delete button to remove the redefined rule from your test configuration.

Update QoS

To add an Update QoS to your **Modify QoS Flow** configuration select the **Add Update QoS** button.



The following table describes the Update QoS settings.

Parameter	Description								
<i>Update QoS Settings:</i>									
	Select the Delete Update QoS button to delete this Update QoS from your objective configuration.								
Flow ID	Select the flow ID from the drop-down list.								
<i>MBR:</i>									
MBR Type	Select the desired Maximum Bit Rate (MBR) type for the flow. Based on your selection, LoadCore will present the appropriate settings.								
<table border="1"> <thead> <tr> <th colspan="2"><i>QoS Rates:</i></th> </tr> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Uplink</td> <td>Set the uplink bitrate.</td> </tr> <tr> <td>Downlink</td> <td>Set the downlink bitrate.</td> </tr> </tbody> </table>		<i>QoS Rates:</i>		Parameter	Description	Uplink	Set the uplink bitrate.	Downlink	Set the downlink bitrate.
<i>QoS Rates:</i>									
Parameter	Description								
Uplink	Set the uplink bitrate.								
Downlink	Set the downlink bitrate.								
<table border="1"> <thead> <tr> <th colspan="2"><i>Dynamic QoS Rates:</i></th> </tr> <tr> <th>Parameter</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>Uplink Action</td> <td>Select the action type to apply to the uplink bitrate.</td> </tr> <tr> <td>Uplink Step</td> <td>Select the step to increase or decrease the uplink bitrate.</td> </tr> </tbody> </table>		<i>Dynamic QoS Rates:</i>		Parameter	Description	Uplink Action	Select the action type to apply to the uplink bitrate.	Uplink Step	Select the step to increase or decrease the uplink bitrate.
<i>Dynamic QoS Rates:</i>									
Parameter	Description								
Uplink Action	Select the action type to apply to the uplink bitrate.								
Uplink Step	Select the step to increase or decrease the uplink bitrate.								

Parameter	Description	
	Downlink Action	Select the action type to apply to the downlink bitrate.
	Downlink Step	Select the step to increase or decrease the downlink bitrate.
<i>Gate Status:</i>		
Uplink	Select an option from the drop-down list. Traffic is forwarded when the gate is open and discarded when the gate is closed.	
Downlink	Select an option from the drop-down list. Traffic is forwarded when the gate is open and discarded when the gate is closed.	

Update URR

To add an Update URR (Usage Reporting Rule) to your **Modify URR Flow** configuration, select the **Add Update URR** button.

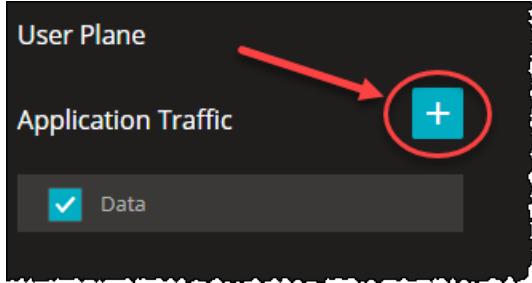
The following table describes the Update URR settings.

Parameter	Description
<i>Update URR Settings:</i>	
	Select the Delete Update URR button to delete this Update URR from your objective configuration.
Flow ID	Select the flow ID from the drop-down list.
<i>Volume Threshold:</i>	
Total	Set the value for the Total Volume field.
Uplink	Set the value for the Uplink Volume field.
Downlink	Set the value for the Downlink Volume field.
<i>Volume Quota:</i>	
Total	Set the value for the Total Volume field.
Uplink	Set the value for the Uplink Volume field.
Downlink	Set the value for the Downlink Volume field.

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.

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



The available traffic applications are: **Stateless UDP**, **Data**, **Voice**, **Video OTT**, **DNS Client** and **Predefined Applications**.

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
Address	The destination IP address for the user plane traffic that this UE range will generate.
	Select this button to add a new application traffic objective. The objective can be: <ul style="list-style-type: none"> Stateless UDP Data Voice Video OTT DNS Client Predefined Applications
	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 .

Parameter	Description
	<u>Traffic.</u>
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <u>Video OTT Traffic.</u>
DNS Client	For the settings required to configure the DNS Client objective, refer to <u>DNS Client Traffic.</u>
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to <u>Predefined Applications Traffic.</u>

Stateless UDP Traffic Generator

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

The following table describes the Stateless UDP parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Flow Type	This field is set to uplink and can not be modified since on the UE you can only configure the uplink flow.
Packet Rate	The rate at which the test generates packets, measured in packets per second (pps).
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The time to wait before the application traffic flows start.
Destination IP Address	The destination IP address to place in the IP packet.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
QoS Flow ID	Select the QoS flow from the drop-down list.
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>

Parameter	Description
Ethernet Device ID	Select the associated ethernet device that will be used to generate this flow.
Destination MAC Address	The destination MAC address to be used for sending this traffic flow as Ethernet traffic encapsulated in GTP. If left blank, ARP or ICMPv6 protocols will be used to learn the destination MAC address.

Data Traffic

The following table describes the Data Traffic parameters.

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

Parameter	Description
Query Per Connection	
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Config on page 256).
QoS FlowID	Select a QoS Flow ID for this flow.

Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Address	The destination IP address for the user plane traffic that this UE range will generate.
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.
Call Type	Select the type of call from the drop-down list. Available options are: <ul style="list-style-type: none"> • Basic Call • Basic Call Mo (Mobile Originated) • Basic Call Mt (Mobile Terminated)
Dial Plan	For the settings required to configure the dial plan, refer to Dial Plan .
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are:

Parameter	Description
	<ul style="list-style-type: none"> TCP - Transmission Control Protocol TLS - Transport Layer Security
<i>RTP Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Media settings:	<i>For the configuration of media settings, refer to Media Settings.</i>

Dial Plan

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

Parameter	Description
Iterations	The number of times the dial plan will be executed. It can be finite or infinite (set to zero).
DNN ID	Select the DNN from the drop-down list.
Source Phone	The phone number assigned to the simulated user.
Destination Phone	The call destination number.
Destination IP	The destination IP address.
Destination Port	The destination port number.

Media Settings

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

Parameter	Description
Audio Duration (ms)	Length of time to play the audio stream. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
<i>Jitter Buffer Settings:</i>	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).

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

AMR/AMR-WD

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> • Bandwidth efficient: In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added. • Octet aligned: In the octet-aligned format, all the fields in a payload, including payload header, table of contents entries, and speech frames themselves, are individually aligned to octet boundaries to make

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

EVS

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

PCMU/PCMA/iLBC/G722/G723/G729

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

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
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Simulated Users, or • Transactions Rate
Transactions rate	<p>IMPORTANT This parameter is available only when Objective Type is set to Transactions Rate.</p> <p>Set the value for the transaction rate parameter.</p>
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.
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. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings. <p>Refer to DNS Client Traffic on the previous page (below) 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.
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 on page 256).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

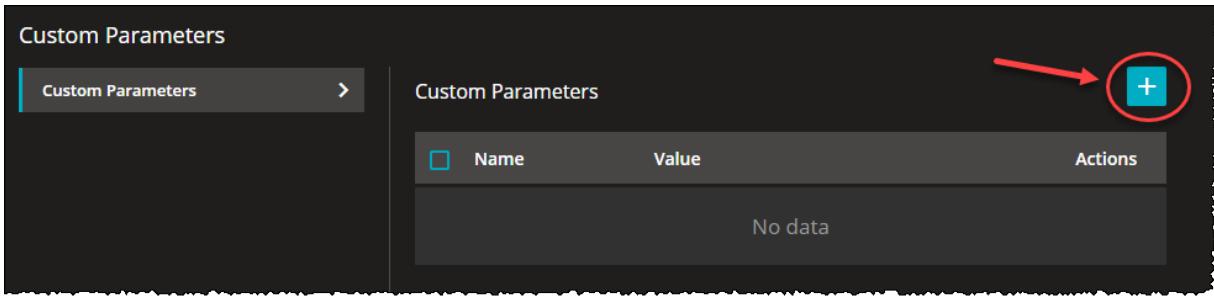
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

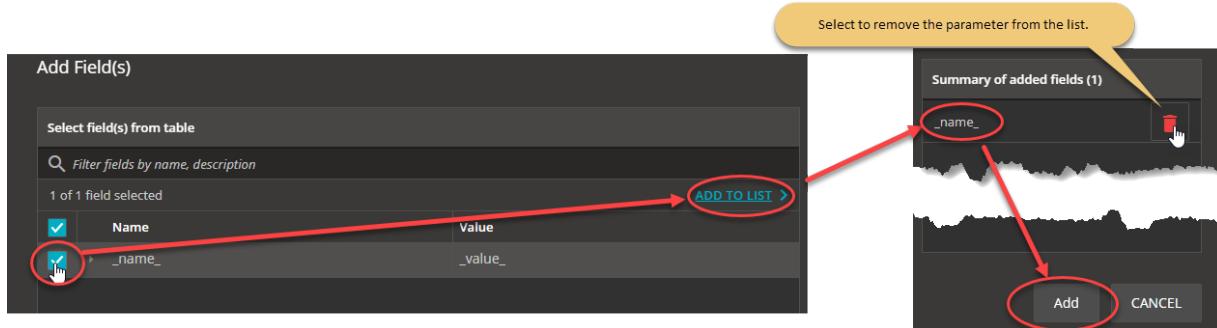
2. Select the **Add** button.



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 ...



Video OTT Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Objective Type	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.
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	<p>Each Application Traffic entry requires at least one Ott 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. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.
<i>Flow:</i>	
	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 APPLE 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
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero).
Percentage	The percentage of total Objective Simulated Users 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(sec)	Set the number of seconds to wait before playback. The default value is 30.
Maximum Size(sec)	Set the number of seconds to be buffered on the client side. The defult value is 500.
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> • Adaptive Bitrate(ABR) • 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 Bitrate .
<i>Play Profiles: The following settings are available and editable only when the Quality Control Mode is set to Quality Predefined Levels.</i>	
	Select this button to add a predefined play profile to your test configuration.
<i>Quality Shift</i>	
	Select this button to remove this play profile from your test configuration.
Shift Type	Select the shift type from the drop-down list. Available options <ul style="list-style-type: none"> • Stay at Current Bitrate • Change to the Lowest Bitrate • Change to the Lowest Bitrate • Change to the Lower Bitrate • Change to the Higher Bitrate
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to Change to Higher Bitrate or Change to Lower Bitrate .
Play Until End	If this check box is selected, the Play Duration field is disabled and the original playtime is used.
Pay duration(sec)	This field is available only if the Play Until End check box is not selected.

Parameter	Description
	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.
Close TCP Connection After Each Transaction	Select the check box to terminate the TCP connection after each transaction.
Enable DNS Query Per Connection.	Select the check box to process only one DNS query per TCP connection.

Predefined Applications Traffic

The following table describes the Predefined Flows Traffic parameters.

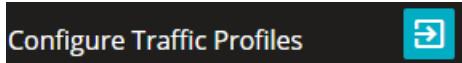
Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Simulated Users • Throughput • Connections Per Second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

Parameter	Description
	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.
Configure Traffic Profiles	Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions. Refer to Traffic Profile on the facing page (below) for a description of the configuration settings for these traffic profiles.

Traffic Profile

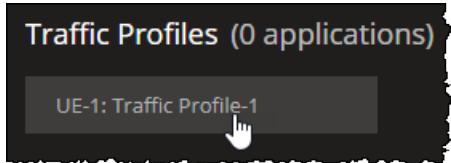
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

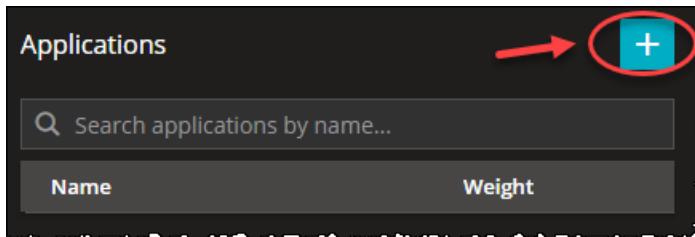
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

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.



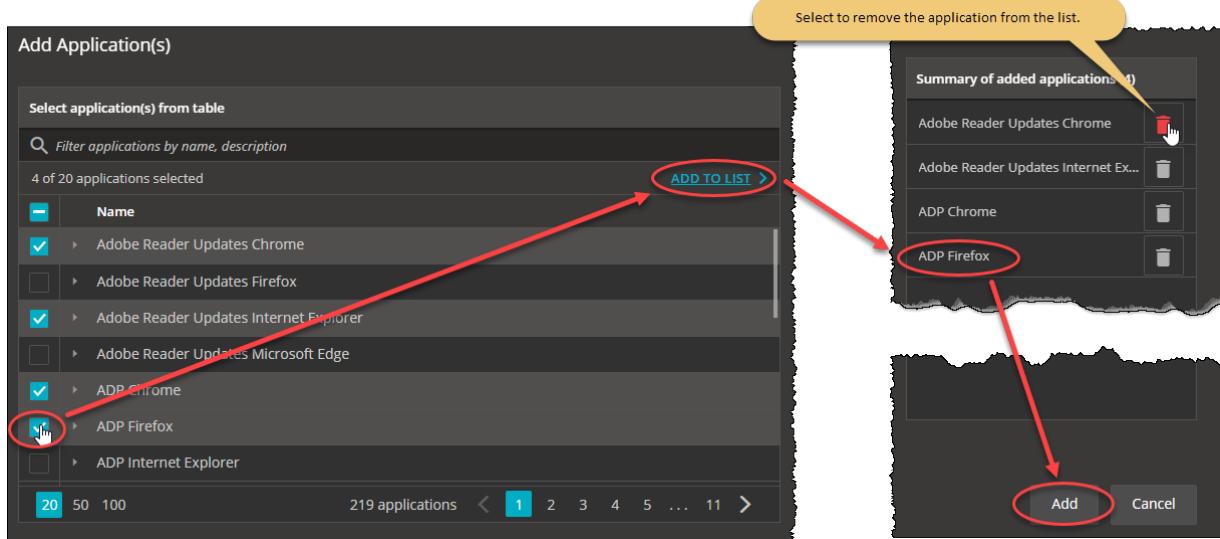
The Add Application(s) window opens.

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 ...

Applications		Edit	+
<input type="text"/> Search applications by name...			
Name	Weight		
Adobe Reader Updates Chrome 1	1	Edit	Delete
Adobe Reader Updates Internet Exp...	1	Edit	Delete
ADP Chrome 3	1	Edit	Delete
ADP Firefox 4	1	Edit	Delete

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

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

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

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

For example ...

The screenshot shows the 'Applications' configuration interface. On the left, there is a list of predefined applications with columns for 'Name' and 'Weight'. One application, 'Adobe Reader Updates Chrome 1', is selected and highlighted with a blue border. On the right, two sections are displayed: 'Application Settings' and 'Application Actions'.

Application Settings

- Destination Hostname: A text input field.
- DNN ID: A dropdown menu set to 'dnn.keysight.com'.
- QoS Flow ID: A dropdown menu set to '1'.

Application Actions

Actions

- A search bar labeled 'Search actions by name...'.
- A table listing actions:

#	Name
1.	Check For Updates Client -> Server acroipm2.adobe.com
2.	Download Updates Client -> Server ardownload.adobe.com

Application Settings

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

NOTE

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

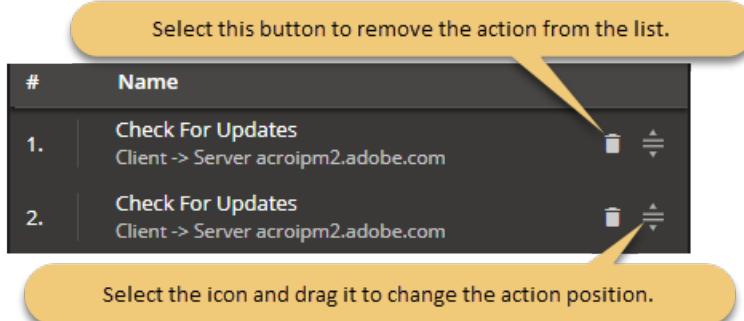
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

Application Actions

The Application Actions section lists the actions and action parameters available in LoadCore 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:

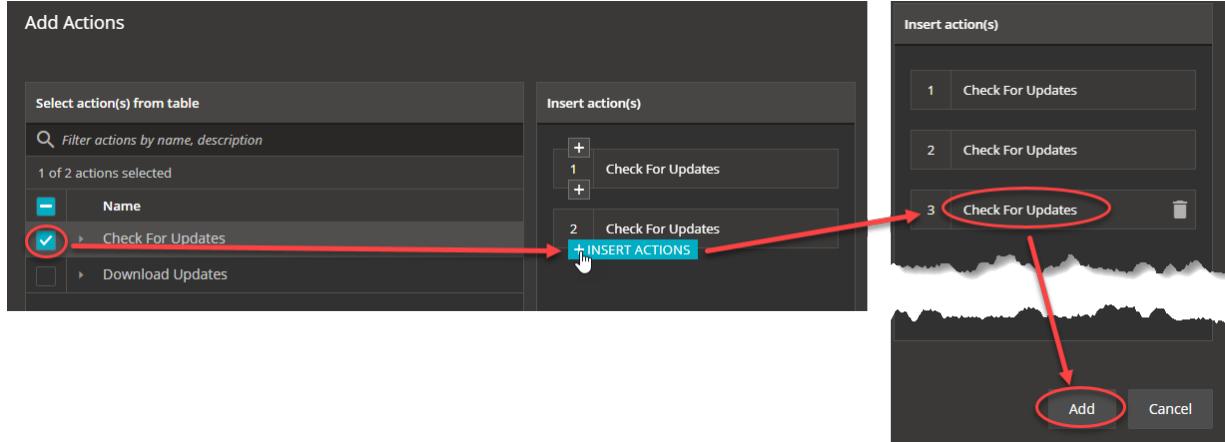
1. Use the icons available for each icon in order to remove it or to change its position in actions list.
For example ...



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 ...



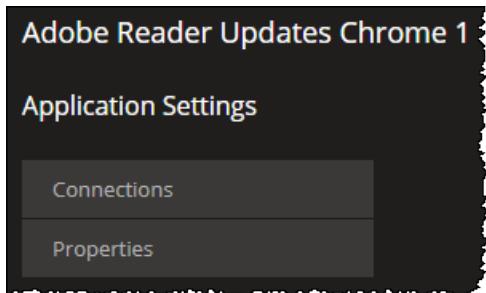
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

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.

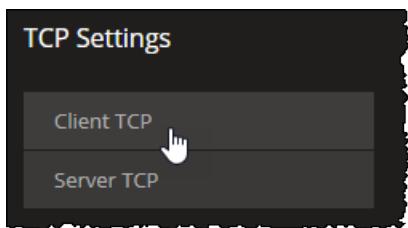
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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

TCP Settings

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



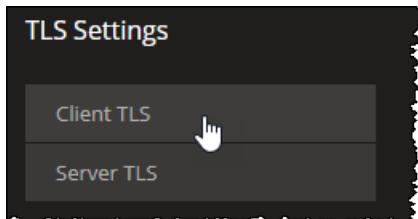
These parameters are configurable for both Client and Server settings, as presented in the following table.

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

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

TLS Settings

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



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
TLSv1.2	Select the check box to enable it. The following options became available:

Parameter	Description
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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> NOTE Session reuse method is available only if TLSv1.2 is selected. </div>
Immediate close	Select the check box to enable it.
TLSv1.3	<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 compatibility	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	Select the check box to enable it.

Server TLS Settings

Parameter	Description
TLSv1.2	<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 style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> NOTE Session reuse method is available only if TLSv1.2 is selected. </div>
Immediate close	Select the check box to enable it.
TLSv1.3	<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	Select the check box to enable it. It allows for compatibility with middleboxes

Parameter	Description
compatibilty	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>
<i>Key file password</i>	<i>Enter your key file password.</i>
<i>DH file Traffic</i>	<i>Select Upload to add your DH file or Clear to remove it.</i>

SMF configuration settings



Session Management Function (SMF), as the name implies, handles management of UE sessions while also allocating IP addresses to UEs. It also selects and controls the UPF for data transfer. Per-session SMFs may be allocated to UEs with multiple sessions. It also interacts with the User Plane Function (UPF) for efficient routing of the user's packets.

SMF interacts with the UPF over the N4 reference point and makes its services available to other network functions through the Nsmf service-based interface.

The configuration settings are described in the topics listed below.

Topics:

SMF Ranges panel	479
SMF Range settings	479
SMF N4 interface settings	480
SMF Uplink Paths	482

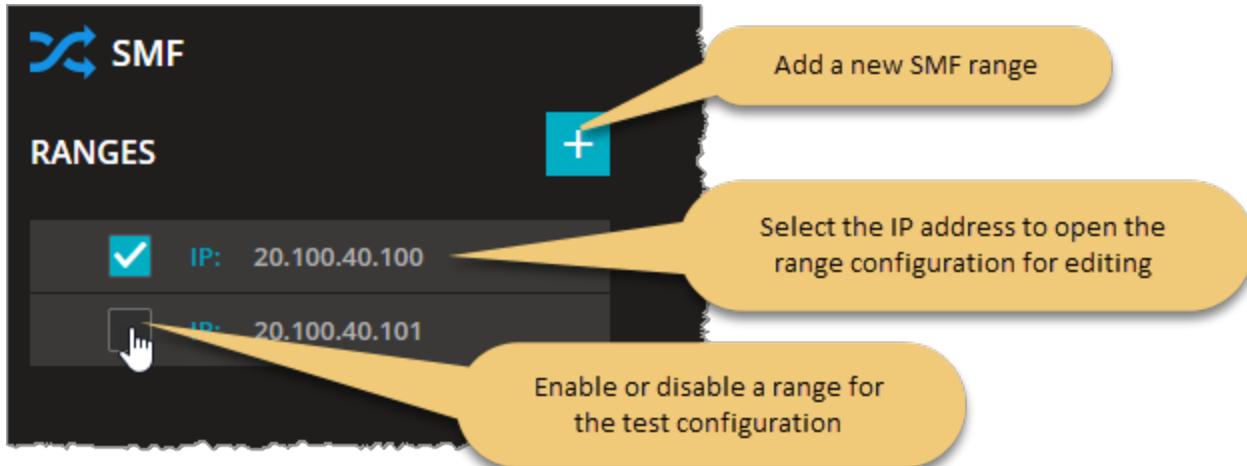
SMF Ranges panel

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

You can perform the following tasks from this panel:

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

For example ...



SMF Range settings

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

- Delete the SMF range from the test configuration.
- Select **Range Settings** to configure the node and connectivity settings for the SMF range.

SMF range controls and settings

Each SMF range is identified by a unique name.

The following table describes the **Range Settings** that you need to configure for each SMF range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Name	The name uniquely identifies the SMF instance. You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Range Settings:</i>	

Setting	Description
N4 Interface Settings	Each SMF range requires the configuration of N4 interface settings, through which a SMF instance interacts with UPF in a 5G network. These settings are described in SMF N4 interface settings below .
Uplink Paths	These settings are described in SMF Uplink Paths on page 482 .

SMF N4 interface settings

N4 is the service-based interface through which a AMF instance interacts with UPF in a 5G network.

The following settings identify the peer node and determine how TEIDs are allocated.

Setting	Description
<i>N4 Interface Settings:</i>	
Peer UPF	Select the UPF node connected to SMF over the N4 interface.
<i>PFCP Settings:</i>	
Use Remote FTEID Allocation	When this option is enabled, SMF expects the UPF to allocate TEIDs. When it is disabled, the UPF allocates TEIDs.
Enable N4u Interface	Select this option to enable the N4u interface on SMF. The SMF uses the same IP on N4 and N4-u.
Include UE IP Address in Access PDI	Select this check box to include the UE IP Address IE in the PDI for Access Source Interface.
Include 3GPP Interface Type	Select this check box to include the 3GPP interface type in PFCP messages.
Include Choose ID	Select this check box to include the Choose ID value in PFCP messages.
Heartbeat Interval	Set the number of seconds between PFCP heartbeat procedures. By default, the value is set to 60, but can be changed using a value between 0 and 3600 (a value of 0 is used to disable such requests).
Session Deletion Rate for UPF triggered Release	This parameter is used to configure the rate for PFCP session deletion when UPF requests PFCP association release. By default, the value is set to 100, but can be changed using a value between 1 and 1.000.000.
Wait for Association Setup	The time in seconds to wait for PFCP Association setup to be initiated by UPF. The default value is 0, meaning the SMF will not wait for UPF to initiate the association.

Setting	Description
	The minimum value is 0 and the maximum value is 3600.
<i>N4-u Settings : These settings are enabled when Enable N4u Interface check box is selected.</i>	
Access SDF	<p>The SDF describing the packet filter. Default value: <i>permit out 58 from any to assigned.</i></p> <p>Example: <i>permit out 17 from 22.22.22.22 11111 to \$ueip\$ 11100</i>. For syntax details refer to TS 29212 5.4.2. <i>\$ueip\$</i> is a format specifier for UE IP address.</p>
CP-Function SDF	<p>The SDF describing the packet filter. Default value: <i>permit out 58 from any to assigned.</i></p> <p>Example: <i>permit out 17 from 22.22.22.22 11111 to \$ueip\$ 11100</i>. For syntax details refer to TS 29212 5.4.2. <i>\$ueip\$</i> is a format specifier for UE IP address.</p>

The following **Connectivity Settings** enable the necessary N4 connectivity and service interaction.

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

SMF Uplink Paths

About uplink paths

The Uplink Path options are used for N9 and ULCL (Uplink Classifier) scenarios. An Uplink Path contains one or more UPFs serving a PDU Session. This is needed because with I-UPF (intermediate UPF) and ULCL (Uplink Classifier) there can be more than one UPF chained between RAN and DN. The rule is that the first UPF in the path is the UPF connected to RAN (N3 UPF) and the last UPF is the UPF connected to DN (N9 UPF).

There are two possible combinations with more than one UPF:

i-UPF:	one N3 UPF (I-UPF) and one N9 UPF	In this case all flows of a PDU session will use the path <i>RAN > N3 UPF > N9 UPF > DN</i> .
ULCL:	one N3 UPF (ULCL) and two N9 UPFs	In this case, some flows defined in the QoS Flows for first N9 UPF will use the path <i>RAN > N3 UPF > First N9 UPF > DN</i> , and others will use <i>RAN > N3 UPF > Second N9 UPF > DN</i> .

Uplink Path settings

The following table describes the settings required to configure the uplink paths.

Setting	Description
<i>Uplink Paths:</i>	
	Select the Add an uplink path button to add an uplink path to your test configuration.
<i>Uplink Path:</i>	
	Select the Delete uplink path button to remove the uplink path from your test configuration.
N3 UPF	Select the first UPF in the path: the UPF connected to the RAN.
<i>Next UPFs:</i>	
First N9 UPF	The first UPF on the N9 interface
QoS Flows for first N9 UPF	Select the QoS Flows for the first N9 UPF.
Second N9 UPF	Select None if your test configures only one N9 UPF or a UPF if you test configures more than one N9 UPF.
QoS Flows for second N9 UPF	Select the QoS Flows for the second N9 UPF.

RAN configuration settings



Radio Access Network (RAN) is the 5G core network component that connects individual devices to other parts of a network through radio connections. A RAN resides between user equipment (UE) and provides the connection with the 5G core network. A RAN provides access and coordinates the management of resources across the radio sites. Multiple instances of RAN may be deployed.

The configuration settings are described in the topics listed below.

Topics:

RAN Ranges panel	484
RAN Range settings	484
RAN N3 interface settings	485
Passthrough interface settings	486

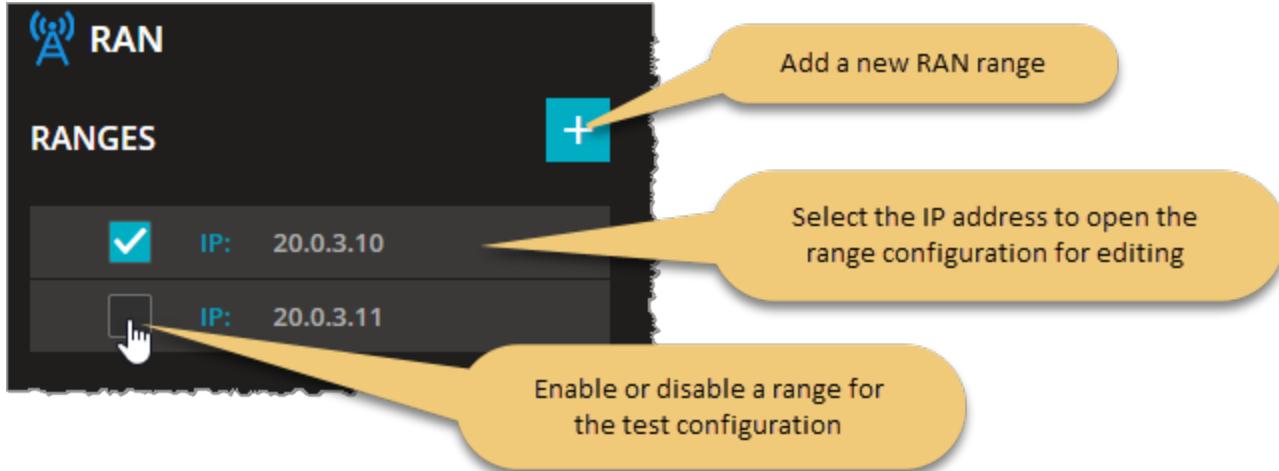
RAN Ranges panel

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

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

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

For example ...



RAN Range settings

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

- Delete the RAN range from the test configuration.
- Select **Range Settings** to configure the node and connectivity settings for the RAN range.

RAN range controls and settings

Each RAN range is identified by a unique name.

The following table describes the **Range Settings** that you need to configure for the RAN range.

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Name	Multiple RAN instances may be deployed in the 5G network. Each RAN instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.

Setting	Description
Range Count	The number of RANs in the RAN range.
<i>Range Settings:</i>	
N3 Interface Settings	Each RAN range requires the configuration of N3 interface settings, through which a RAN instance enables connectivity and interaction with the UPF component in the 5G network. These settings are described in RAN N3 interface settings below .
Passthrough Interface Settings	These settings are described in Passthrough interface settings on the next page .

RAN N3 interface settings

The following configuration settings are required by the RAN N3 interface .

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 the this node.
Gateway Address	The IP address assigned as gateway address.
MTU	Maximum transmission unit.
MSS	Maximum segment size.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT <i>This option is visible only when the Outer VLAN check-box is selected.</i></p> <p><i>Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.</i></p>

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

Passthrough interface settings

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.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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 assigned as the gateway address for the external traffic source.
IP Prefix Length	The IP address prefix length.
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.
Inner VLAN	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.

UPF configuration settings

The configuration settings are described in the topics listed below.

Topics:

UPF Ranges panel	488
UPF Range panel	488
UPF N3 interface settings	489
UPF N4 interface settings	490
UPF N6 interface settings	492
UPF N9 interface settings	493
UPF N4u interface settings	494

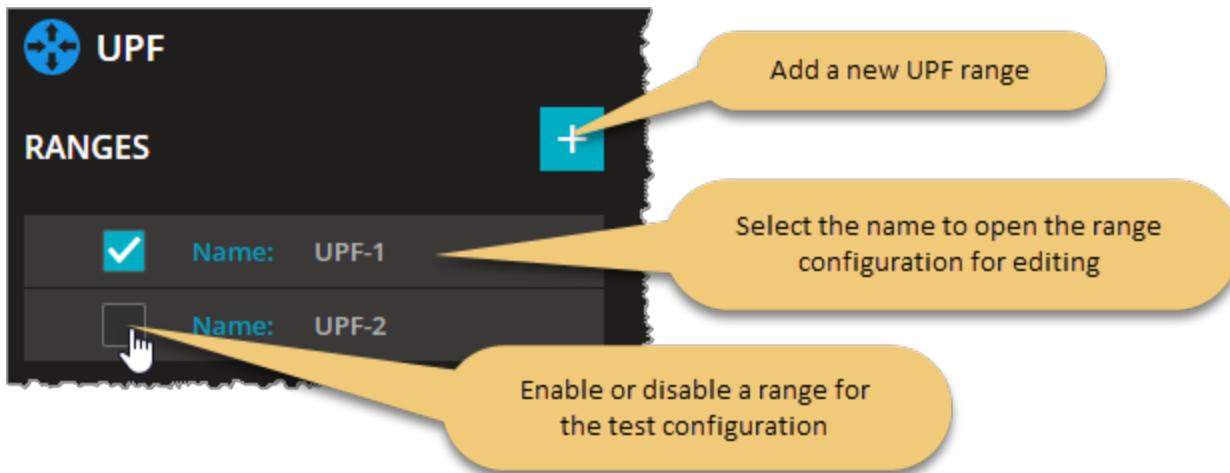
UPF Ranges panel

The **UPF/PGW-U Ranges** panel opens when you select the UPF/PGW-U node from the network topology window.

You can perform the following tasks from this 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 ...



UPF Range panel

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

- Delete the UPF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Modify the UPF range **Name**.
- Configure interface settings for the UPF range.

The following table describes the **Range Settings** that you need to configure for each UPF 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 UPF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the UPF functionality (if it is selected in the Topology window).

Setting	Description
Name	The name of the UPF range. You can accept the name provided by the LoadCore, or you can replace it with a name of your own choosing.
Range Count	The number of UPFs in the UPF range.
<i>Range Settings:</i>	
N3 Interface Settings	N3 is the interface between the RAN and the UPF. The interface settings are described in UPF N3 interface settings below .
N4 Interface Settings	N4 is the interface between the SMF and the UPF. The interface settings are described in UPF N4 interface settings on the next page .
N6 Interface Settings	N6 is the interface between the DN and the UPF. The interface settings are described in UPF N6 interface settings on page 492 .
N9 Interface Settings	N9 is the interface between two UPFs. The interface settings are described in UPF N9 interface settings on page 493 .
N4u Interface Settings	N4u is an interface between the SMF and the UPF. The interface settings are described in UPF N4u interface settings on page 494 .

UPF N3 interface settings

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

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

Setting	Description
<i>N3 Interface Settings:</i>	
Network Instance	The network domain that will be used in the Network Instance information element (IE) in messages sent on this interface. The UPF uses the Network Instance to determine the IP network to use when transferring traffic over the N3 interface.
<i>Network Instance:</i>	
	Select the Add value button to add a network instance to your test configuration.
	Select the Delete button to remove the network instance from your test configuration.
Network Instance Format	Select the encoding format for the network instance: string or label-list.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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.
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.
<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.

UPF N4 interface settings

The UPF receives user traffic information from the SMF over the N4 interface. N4—which employs the Packet Forwarding Control Protocol (PFCP)—is the control plane interface between the UPF and the SMF. PFCP sessions established with the UPF define how packets are identified, forwarded, processed, marked, and reported (using PDRs, FARs, BARs, QERs, and URRs).

The following configuration settings are required by each UPF N4 range.

Setting	Description
<i>N4 Interface Settings:</i>	
Peer SMF	<p>By default, the value is set to None. This means that UPF expects the PFCP Association to be initiated by the SMF node.</p> <p>If this field is populated with one of the SMF nodes configured in the test (available in the drop-down list), then the UPF, upon startup, will try to establish the PFCP Association with the configured SMF.</p>
<i>PFCP Settings:</i>	
Supports FTEID Allocation	When this option is enabled, the UPF allocates TEIDs. When it is disabled, the UPF expects the SMF to allocate TEIDs.
Heartbeat Interval	Set the number of seconds between PFCP heartbeat procedures. By default, the value is set to 60, but can be changed using a value between 0 and 3600 (a value of 0 is used to disable such requests).
Release PFCP association before node stop	When selected, the UPF will send PFCP Association Update to release PFCP association before UPF node stop.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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.
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</i>

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

UPF N6 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** are required by each UPF N6 range.

NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
MTU	Maximum transmission unit.
MSS	Maximum segment size.
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</i>

Connectivity Settings	Description
	VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p>IMPORTANT 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.

UPF N9 interface settings

N9 is the interface between two UPFs in a 5G network: for example an I-UPF and the UPF session anchor. An I-UPF performs a relay function, while the session anchor terminates the protocols (such as GTP) used on that interface.

You can enable or disable the N9 interface, as required by your test configuration. For example:



Interface Settings	Description
Network Instance	The network domain that will be used in the Network Instance information element (IE) in messages sent on this interface. The UPF uses the Network Instance to determine the IP network to use when transferring traffic over the N9 interface.
<i>Add Network Instance:</i>	
	Select the Add value button to add a network instance to your test configuration.
	Select the Delete button to remove the network instance from your test configuration.
Network Instance Format	Select the encoding format for the network instance: string or label-list.

The following **Connectivity Settings** enable the necessary N9 connectivity between UPF nodes.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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.
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.
<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.

UPF N4u interface settings

The N4u interface is used to forward packets between SMF and UPF. It is used only for SLAAC.

The UPF can use the same or different IPs on N4 and N4-u.

You can enable or disable the N4u interface, as required by your test configuration. For example:



Interface Settings	Description
Network Instance	The network domain that will be used in the Network Instance information element (IE) in messages sent on this interface. The UPF uses the Network Instance to determine the IP network to use when transferring traffic over the N4u interface.
<i>Add Network Instance:</i>	
	Select the Add value button to add a network instance to your test configuration.
	Select the Delete button to remove the network instance from your test configuration.
Network Instance Format	Select the encoding format for the network instance: string or label-list.

Connectivity Settings

The following **Connectivity Settings** enable the necessary N4u connectivity between the UPF and SMF.

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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

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

DN configuration settings



Data Networks (DN) represents one of the entities in the 5G core network architecture. DN interfaces with UPF over the N6 reference point, enabling access to the public Internet, operator services, and other external data networks.

The configuration settings are described in the topics listed below.

Topics:

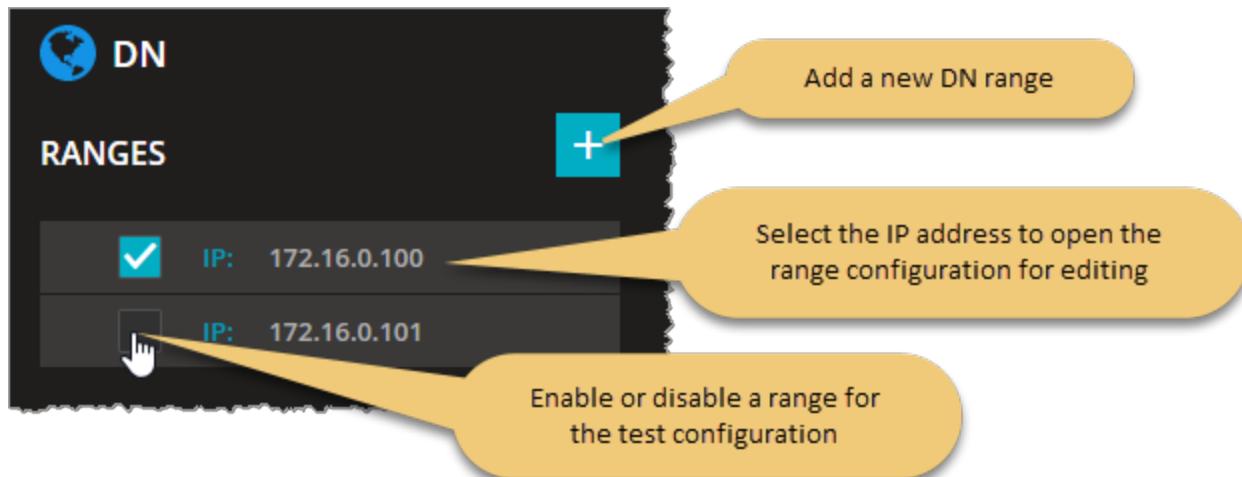
DN Ranges panel	497
DN Range panel	497
DN N6 Interface settings	498
DN UE routes settings	499
DN User Plane	500
DN Application Traffic Generator	500
DN Stateless UDP Traffic Generator	507

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 **DN Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- Select the **Delete Range** button to delete the DN range from the test configuration.
- Select **N6 Interface Settings** to configure the DN connectivity settings for the DN range.
- Select **UE Routes Settings** to configure the route to an UE range.
- Select **User Plane** to configure the traffic generators.

N6 Interface settings

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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Range Count	The number of DNs in the DN range.
<i>Range Settings:</i>	
N6 Interface Settings	Each DN range requires the configuration of N6 interface settings, through which a DN instance enables connectivity and interaction with other functions in the 5G network. These settings are described in DN N6 Interface settings below .
UE Routes Settings	These settings are described in DN UE routes settings on the facing page .
User Plane	These settings are described in DN User Plane on page 500 .

DN N6 Interface settings

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

NOTE

The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

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

DN UE routes settings

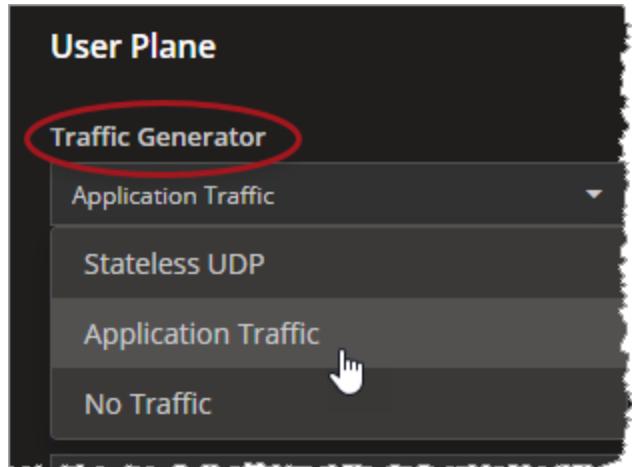
The following table describes the **UE Route Settings** that you need to configure in order to create the route to an UE range.

Settings	Description
<i>UE Routes Config:</i>	
	Select this button to add a new route to a specific UE range.
<i>UE Routes Config:</i>	
	Select this button to remove the route to the UE range.

Settings	Description
UE Range IP	Select the IP 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.

DN User Plane

LoadCore provides two traffic generators: **Application Traffic** and **Stateless UDP** (plus a **No Traffic** option for tests that do not require user plane traffic):



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](#).

The DN settings required for the traffic generators are described in the following topics:

- [DN Application Traffic Generator](#)
- [DN Stateless UDP Traffic Generator on page 129](#)

DN Application Traffic Generator

Use the **Application Traffic** generator to generate IP packets containing Layer 7 traffic for your test.



You can choose to generate Data Traffic, Voice Traffic or Ott Traffic, based on your test requirements.

The following table describes the Application Traffic generation parameters.

Parameter	Description
Address	The destination IP address for the user plane traffic that this UE range will generate.
	Select this button to add a new application traffic objective. The objective can be either Data , Voice or Ott .
	Select this button to remove the application traffic objective from your test configuration.
Data	For the settings required to configure the Data traffic objective, refer to DN Data Traffic .
Voice	For the settings required to configure the Voice traffic objective, refer to DN Voice Traffic .
Ott	For the settings required to configure the Ott traffic objective, refer to DN Ott Traffic .

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 .
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).
Application Traffic Flows	Each Application Traffic entry requires at least one 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. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings. Refer to Flow on the next page (below) for a description of the configuration settings for these traffic flows.

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	Select the L4/L7 protocol type from the list of pre-defined flows. The available Types include: <ul style="list-style-type: none"> • HTTP Get and HTTP Put • HTTPS Get and HTTPS Put • FTP • UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)
Port	The port used by the 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.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional.

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 .
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated 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).
Call Type	Select the type of call from the drop-down list. Available options are: <ul style="list-style-type: none"> • Basic Call

Parameter	Description
	<ul style="list-style-type: none"> • Basic Call Mo (Mobile Originated) • Basic Call Mt (Mobile Terminated)
Dial Plan:	<i>For the settings required to configure the dial plan, refer to Dial Plan.</i>
<i>Sip Settings:</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore 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
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Media settings:	<i>For the configuration of media settings, refer to Media Settings.</i>

Dial Plan

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

Parameter	Description
Iterations	The number of times the Voice flow will be executed. It can be finite or infinite (set to zero).
Source Phone	The URI assigned to the first simulated user, incremented by 1 for each UE.
Destination Phone	The URI assigned to the first simulated user, incremented by 1 for each UE.
Destination IP	The destination IP address.
Destination Port	The destination port number.

Media Settings

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

Parameter	Description
Audio Duration (ms)	Length of time to play the audio stream. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID	The QoS Flow ID for RTP traffic. Select the QoS Flows ID(s) 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-WD

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

Parameter	Description
Payload Type	Specifies the audio payload type.
Payload Format	<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.

DN Ott Traffic

The following table describes the 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 Ott .
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>OTT Servers:</i>	
	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 LoadCore or overwrite it with your own value.
Transport	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • HTTP • HTTPS
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Streams:</i>	
	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 LoadCore 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

Parameter	Description
	<ul style="list-style-type: none"> Synthetic
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. 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. 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. If the stream type is set to Real, you will see the real segment duration.</p>
Quality Levels:	<p><i>Set the quality value for each level. The available options are: 500, 1000, 3000 and 5000 Kbps.</i></p> <p><i>If the stream type is set to Synthetic, you can configure maximum 8 quality levels specifying their bitrate in Kbps.</i></p> <p><i>If the stream type is set to Real, you will see the quality levels from the real stream.</i></p>
	Select this button to add a quality level to your test configuration.
	Select this button to remove the quality level from the test configuration.

DN Stateless UDP Traffic Generator

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
<i>Stateless UDP Flows:</i>	
	Select the Add Flow button to add a downlink flow to the Stateless UDP Flows list.
<i>Flow:</i>	
	Select the Delete Flow button to remove this flow from the Stateless UDP Flows list.
Type	This field is set to downlink and can not be modified since on the DN you can only

Parameter	Description
	configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Payload Size	The size of the packet payload, in bytes.
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	Select the DNN value for the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
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>

CHAPTER 10

Passthrough testing

Although LoadCore is designed to internally generate simulated IP traffic, it also enables a test environment in which you configure external traffic sources in your test network. This is called passthrough testing because the external traffic is transmitted to and processed by the LoadCore test engine, bypassing the internal IP traffic generation process (*Objectives* configuration).

Topics:

Overview of passthrough testing	510
Passthrough test configuration notes	511

Overview of passthrough testing

Supported test topologies

The following LoadCore test types (topologies) support the use of passthrough testing:

- Full Core
- NG-RAN Simulation
- UPF Isolation

Functional overview

In each supported test topology, you can configure passthrough on the NG-RAN and on the UPF (and also on the SMF in the UPF Isolation topology). A given test may configure either or both. The following steps give a summary of the test setup and execution when both passthrough interfaces are configured.

1. Create a new test or modify a previously-created test.
2. Configure a passthrough interface on the NG-RAN.
This is the interface on which the NG-RAN will receive traffic from your external traffic source.
3. Configure a UE range with the IP address set to your external traffic source.

NOTE

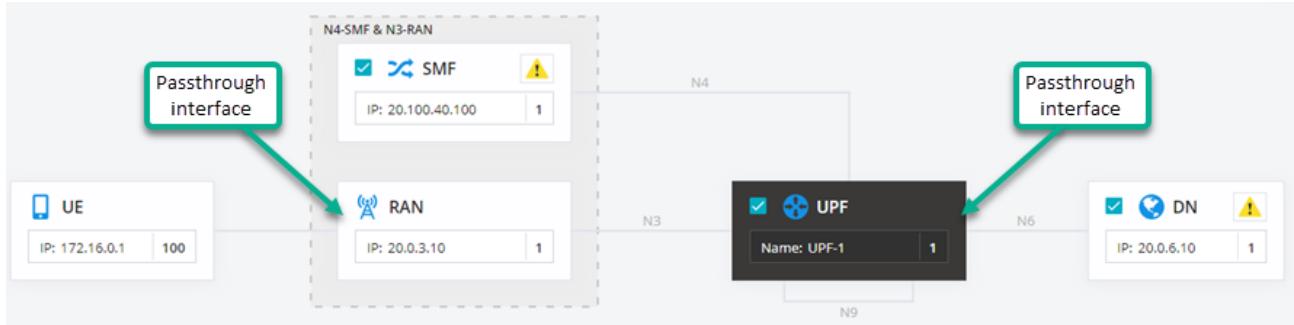
Both passthrough traffic and User Plane objectives traffic can work simultaneously. If you want only passthrough traffic, then there is no need to configure any traffic objectives.

NOTE

The passthrough functionality does not support DPDK devices, its performance is limited (max 1Gbps throughput) and should only be used for functionality testing. Also, all packets coming through the passthrough device will be mapped only on the default flow.

4. Configure a passthrough interface on the UPF.
This is the N6 interface over which the UPF sends packets to and receives packets from your external DN node.
5. Configure network routes on the traffic generators. If you are using the LoadCore sgi-client/sgi-server applications as traffic generators, the network routes must be added via REST API. If you are using third-party traffic generators, you must make sure that the network routes are configured correctly.
6. Once the test starts, the NG-RAN receives IP packets from your external traffic source, encapsulates the packets (adding a GTP-U header), and forwards them over the N3 interface towards the UPF.
7. The UPF removes the GTP-U header from the packets and forward them over the N6 interface towards the external DN node.
8. Your external DN node generates IP packets and forwards them to the UPF over the N6 interface.
9. The UPF encapsulates the packets (adding GTP-U headers) and forwards them over the N3 interface towards the NG-RAN, where they will be decapsulated and sent to the destination node.

The following illustration shows the location of the passthrough interfaces in the UPF Isolation topology:



Passthrough test configuration notes

This topic summarizes the test configuration actions that are unique to and required by passthrough tests.

- [RAN settings below](#)
- [UE settings below](#)
- [UPF settings on the next page](#)
- [N4-SMF & N3-RAN settings on the next page](#)
- [For more information on the next page](#)

RAN settings

The RAN settings are the same for each of the test types that support passthrough testing.

 RAN	<ul style="list-style-type: none"> • From the RAN Range Settings, select Passthrough Interface Settings, then select the Connectivity Settings. The <i>IP Address</i> that you configure will be the IP gateway address for the traffic sent from the external traffic source. • From the topology window, select the agent icon to open the RAN Agent Assignment window. In the Passthrough Device column, select a device that is not used by another interface in that test. This is the device from which the traffic is sent.
---	---

UE settings

The UE settings are the same for each of the test types that support passthrough testing.

 UE	<ul style="list-style-type: none"> • From the UE Range Settings, select Settings, then select the <i>Enable Passthrough</i> option. • Configure Objectives if you want to simultaneously send Objectives-defined traffic and passthrough traffic. If you want to send only passthrough traffic, then there is no need to configure Objectives.
--	--

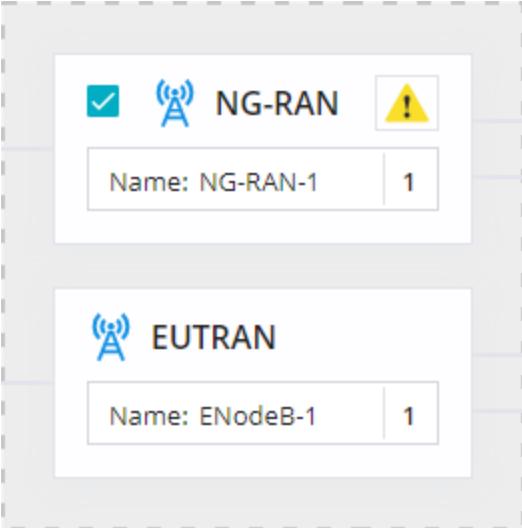
UPF settings

The UPF settings are the same for each of the test types that support passthrough testing.

 UPF	<ul style="list-style-type: none"> From the UPF Range Settings, select N6 Interface Settings, then select the Connectivity Settings. The <i>IP Address</i> that you configure will be the IP gateway address for the external server. From the topology window, select the agent icon to open the UPF Agent Assignment window. In the N6 column, select a device that is the DN destination for the traffic originating from the external client node. Select a device that is not used by another interface in that test.
--	---

N4-SMF & N3-RAN settings

The UPF Isolation test type supports configuration of a passthrough interface, as follows:

	<ul style="list-style-type: none"> From the RAN Range Settings, select Passthrough Interface Settings, then select the Connectivity Settings. The <i>IP Address</i> that you configure will be the IP gateway address for the traffic sent from the external traffic source. From the topology window, select the agent icon to open the Agent Assignment window. In the Passthrough Device column, select a device for this interface.
--	--

For more information

Full Core topology:

- [Passthrough interface settings on page 185](#)
- [UE Settings settings on page 249](#)
- [UPF N6 interface settings on page 231](#)

UPF Isolation:

- [Passthrough interface settings on page 486](#)
- [UE range settings on page 435](#)
- [UPF N6 interface settings on page 492](#)

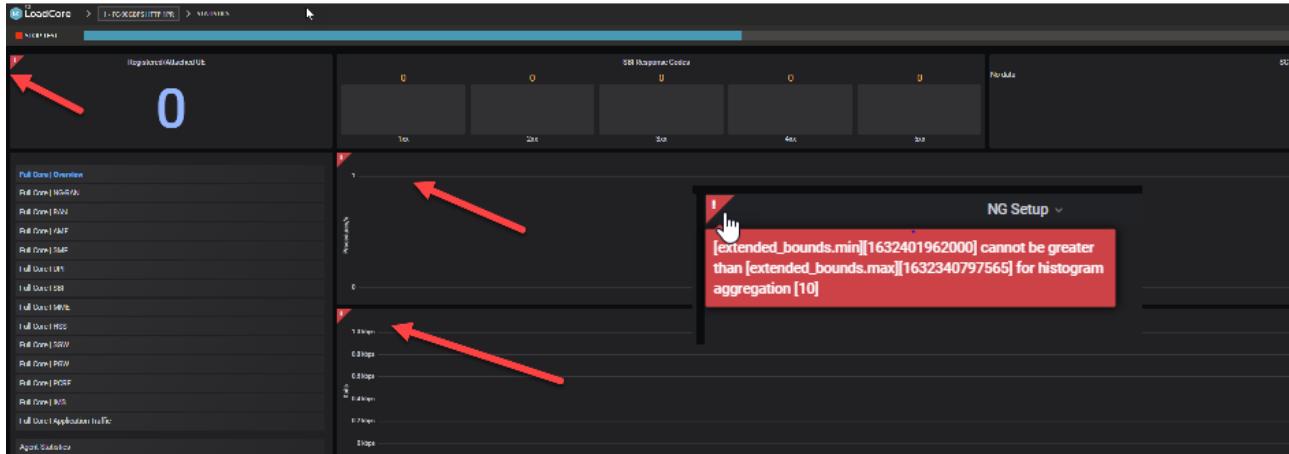
CHAPTER 11

Troubleshooting

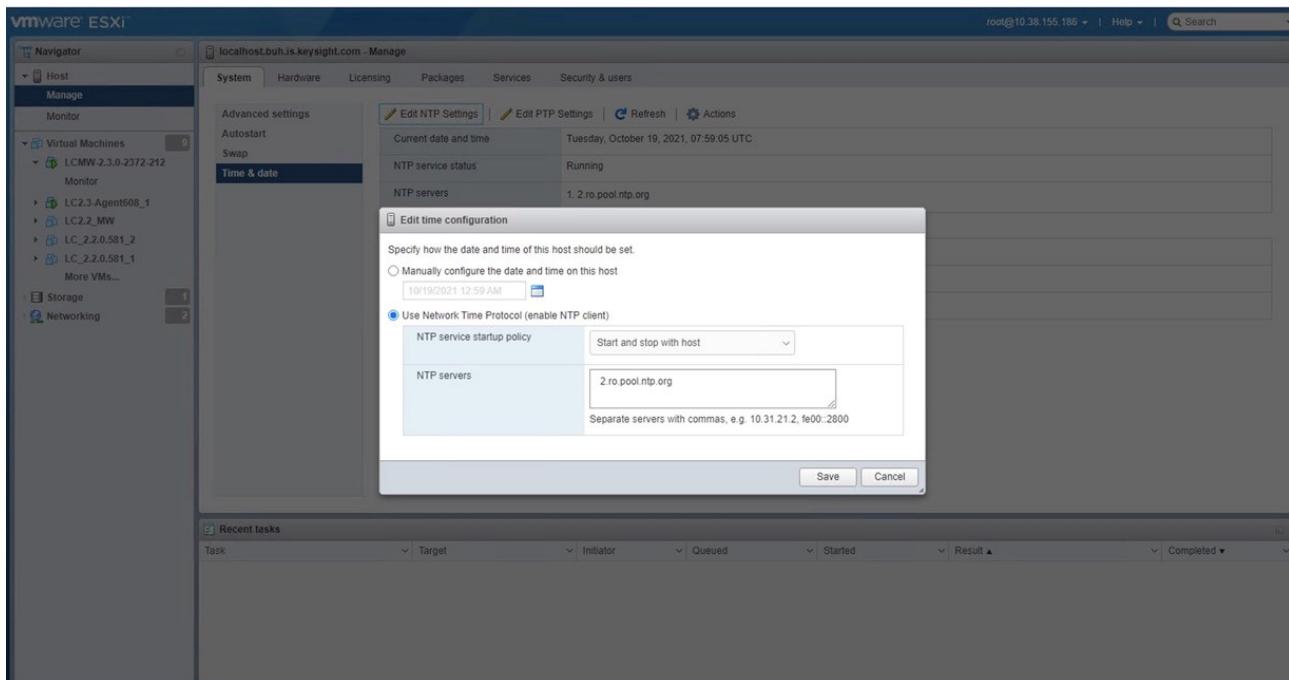
This section presents the most common errors or issues and their associated resolution (if available).

NTP issue

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 LoadCore 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 `btpservice` 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.

APPENDIX A

5G abbreviations

The following list of abbreviations is based on the 3GPP technical specifications.

Abbreviation	Description
5GC	5G Core Network
5GS	Fifth Generation System
5G-AN	5G Access Network
5G-EIR	5G-Equipment Identity Register
5G-GUTI	5G Globally Unique Temporary Identifier
5G-S-TMSI	5G S-Temporary Mobile Subscription Identifier
5QI	5G QoS Identifier
ADC	Application Detection and Control
AF	Application Function
AMBR	Aggregate Maximum Bit Rate
AMF	Access and Mobility Management Function
AN	Access Network
ARP	Allocation Retention Priority
AS	Access Stratum
AUSF	Authentication Server Function
BAR	Buffering Action Rule
BSF	Binding Support Function
CAPIF	Common API Framework for 3GPP northbound APIs
CHF	Charging Function
CIDR	Classless Inter-Domain Routing

Abbreviation	Description
CN	Core Network
CP	Control Plane
DL	Downlink
DN	Data Network
DNAI	Data Network Access Identifier
DNN	Data Network Name
DRX	Discontinuous Reception
E-UTRAN	Evolved UMTS Terrestrial Radio Access Network (LTE)
EBI	EPS Bearer Identity
eMBB	enhanced Mobile Broadband
ePDG	evolved Packet Data Gateway
FAR	Forwarding Action Rule
FQDN	Fully Qualified Domain Name
F-TEID	Fully-qualified Tunnel Endpoint Identifier
GBR	Guaranteed Bit Rate
GFBR	Guaranteed Flow Bit Rate
GMLC	Gateway Mobile Location Centre
gNB	Fifth generation NodeB (gNode)
GPSI	Generic Public Subscription Identifier
GSM	Global System for Mobile communications
GUAMI	Globally Unique AMF Identifier
HPLMN	Home Public Land Mobile Network
HR	Home Routed (roaming)
I-UPF	Intermediate UPF
IMS	IP Multimedia Subsystem
iRAT	inter-RAT (Radio Access Technology)

Abbreviation	Description
ITU	International Telecommunication Union
LADN	Local Area Data Network
LBO	Local Break Out (roaming)
LMF	Location Management Function
LRF	Location Retrieval Function
MBR	Maximum Bit Rate
MCX	Mission Critical Service
MDBV	Maximum Data Burst Volume
MEC	Multi-access Edge Computing (also, Mobile Edge Computing)
MFBR	Maximum Flow Bit Rate
MICO	Mobile Initiated Connection Only
MPS	Multimedia Priority Service
MSISDN	Mobile Station International Subscriber Directory Number
N3IWF	Non-3GPP InterWorking Function
NAI	Network Access Identifier
NAS	Non Access Stratum
NEF	Network Exposure Function
NF	Network Function
NGAP	Next Generation Application Protocol
NR	New Radio
NRF	Network Repository Function
NSI	ID Network Slice Instance Identifier
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSP	Network Slice Selection Policy
NVF	Network Function Virtualization

Abbreviation	Description
NWDAF	Network Data Analytics Function
PCC	Policy and Charging Control
PCF	Policy Control Function
PDN	Packet Data Network
PDR	Packet Detection Rule
PDU	Protocol Data Unit
PEI	Permanent Equipment Identifier
PER	Packet Error Rate
PFCP	Packet Forwarding Control Protocol
PFD	Packet Flow Description
PLMN	Public Land Mobile Network
PPD	Paging Policy Differentiation
PPF	Paging Proceed Flag
PPI	Paging Policy Indicator
PSA	PDU Session Anchor
SCP	Service Communication Proxy
QCI	QoS Class Identifier
QER	QoS Enforcement Rule
QFI	QoS Flow Identifier
QoE	Quality of Experience
QoS	Quality of Service
(R)AN	(Radio) Access Network
RAT	Radio Access Technology
RQA	Reflective QoS Attribute
RQI	Reflective QoS Indication
RRC	Radio Resource Control

Abbreviation	Description
RTP	Real-time Transport Protocol
SA NR	Standalone New Radio
SBA	Service Based Architecture
SBI	Service Based Interface
SCTP	Stream Control Transmission Protocol
SD	Slice Differentiator
SDAP	Service Data Adaptation Protocol
SDF	Service Data Flow
SDM	Subscriber Data Management
SDN	Software-Defined Networking
SEAF	Security Anchor Functionality
SEPP	Security Edge Protection Proxy
SLAAC	Stateless Address Auto-configuration
SMF	Session Management Function
SMSF	Short Message Service Function
S-NSSAI	Single Network Slice Selection Assistance Information
SPGW	Serving/Packet Data Network Gateway
SSC	Session and Service Continuity
SST	Slice/Service Type
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TA	Tracking Area
TAC	Tracking Area Code
TAI	Tracking Area Identity
TEID	Tunnel Endpoint Identifier
TNL	Transport Network Layer

Abbreviation	Description
TNLA	Transport Network Layer Association
TSP	Traffic Steering Policy
UDM	Unified Data Management
UDR	Unified Data Repository
UDSF	Unstructured Data Storage Function
UL	Uplink
ULCL	Uplink Classifier
UP	User Plane
UPF	User Plane Function
URR	Usage Reporting Rules
URSP	UE Route Selection Policy
USIM	UMTS Subscriber Identify Module
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VoNR	Voice over New Radio

APPENDIX B

Predefined Applications

The following table describes the available Predefined Applications.

Application	Description
Adobe Reader Updates Chrome	This application simulates Adobe Reader Updates web application with the Google Chrome browser.
Adobe Reader Updates Firefox	This application simulates Adobe Reader Updates web application with the Google Firefox browser.
Adobe Reader Updates Internet Explorer	This application simulates Adobe Reader Updates web application with the Google Internet Explorer browser.
Adobe Reader Updates Microsoft Edge	This application simulates Adobe Reader Updates web application with the Google Microsoft Edge browser.
ADP Chrome	This application simulates ADP web application with the Chrome browser.
ADP Firefox	This application simulates ADP web application with the Firefox browser.
ADP Internet Explorer	This application simulates ADP web application with the Internet Explorer browser.
ADP Microsoft Edge	This application simulates ADP web application with the Microsoft Edge browser.
Airbnb Chrome	This application simulates Airbnb web application with the Google Chrome browser.
Airbnb Firefox	This application simulates Airbnb web application with the Mozilla Firefox browser.
Airbnb Internet Explorer	This application simulates Airbnb web application with the Internet Explorer browser.
Airbnb Microsoft Edge	This application simulates Airbnb web application with the Microsoft Edge browser.
appointy Chrome	This application simulates appointy web application with the Chrome browser.
appointy Firefox	This application simulates appointy web application with the Firefox browser.
appointy Internet Explorer	This application simulates appointy web application with the Internet Explorer browser.
appointy Microsoft	This application simulates appointy web application with the Microsoft Edge browser.

Application	Description
Edge	browser.
AWS Console Chrome	This application simulates AWS Console web application with the Chrome browser.
AWS Console Firefox	This application simulates AWS Console web application with the Firefox browser.
AWS Console Internet Explorer	This application simulates AWS Console web application with the Internet Explorer browser.
AWS Console Microsoft Edge	This application simulates AWS Console web application with the Microsoft Edge browser.
AWS S3 Chrome	This application simulates AWS S3 web application with the Google Chrome browser.
AWS S3 Firefox	This application simulates AWS S3 web application with the Mozilla Firefox browser.
AWS S3 Internet Explorer	This application simulates AWS S3 web application with the Internet Explorer browser.
AWS S3 Microsoft Edge	This application simulates AWS S3 web application with the Microsoft Edge browser.
Baidu Chrome	This application simulates Baidu web application with the Chrome browser.
Baidu Firefox	This application simulates Baidu web application with the Firefox browser.
Baidu Internet Explorer	This application simulates Baidu web application with the Internet Explorer browser.
Baidu Maps Chrome	This application simulates Baidu Maps web application with the Google Chrome browser.
Baidu Maps Firefox	This application simulates Baidu Maps web application with the Mozilla Firefox browser.
Baidu Maps Internet Explorer	This application simulates Baidu Maps web application with the Internet Explorer browser.
Baidu Maps Microsoft Edge	This application simulates Baidu Maps web application with the Microsoft Edge browser.
Baidu Microsoft Edge	This application simulates Baidu web application with the Microsoft Edge browser.
Bilibili Chrome	This application simulates Bilibili web application with the Google Chrome browser.

Application	Description
Bilibili Firefox	This application simulates Bilibili web application with the Mozilla Firefox browser.
Bilibili Internet Explorer	This application simulates Bilibili web application with the Internet Explorer browser.
Bilibili Microsoft Edge	This application simulates Bilibili web application with the Microsoft Edge browser.
Cisco Spark Chrome	This application simulates Cisco Spark web application with the Chrome browser.
Cisco Spark Firefox	This application simulates Cisco Spark web application with the Firefox browser.
Cisco Spark Internet Explorer	This application simulates Cisco Spark web application with the Internet Explorer browser.
Cisco Spark Microsoft Edge	This application simulates Cisco Spark web application with the Microsoft Edge browser.
Commvault Chrome	This application simulates Commvault web application with the Google Chrome browser.
Commvault Firefox	This application simulates Commvault web application with the Mozilla Firefox browser.
Commvault Internet Explorer	This application simulates Commvault web application with the Internet Explorer browser.
Commvault Microsoft Edge	This application simulates Commvault web application with the Microsoft Edge browser.
Crawling Wikipedia (Chinese) Chrome	This application simulates Crawling Wikipedia (Chinese) web application with the Chrome browser.
Crawling Wikipedia (Chinese) Firefox	This application simulates Crawling Wikipedia (Chinese) web application with the Firefox browser
Crawling Wikipedia (Chinese) Internet Explorer	This application simulates Crawling Wikipedia (Chinese) web application with the Internet Explorer browser.
Crawling Wikipedia (Chinese) Microsoft Edge	This application simulates Crawling Wikipedia (Chinese) web application with the Microsoft Edge browser.

Application	Description
DocuSign Chrome	This application simulates DocuSign web application with the Google Chrome browser.
DocuSign Firefox	This application simulates DocuSign web application with the Mozilla Firefox browser.
DocuSign Internet Explorer	This application simulates DocuSign web application with the Internet Explorer browser.
DocuSign Microsoft Edge	This application simulates DocuSign web application with the Microsoft Edge browser.
Dreambox Chrome	This application simulates Dreambox web application with the Google Chrome browser.
Dreambox Firefox	This application simulates Dreambox web application with the Mozilla Firefox browser.
Dreambox Internet Explorer	This application simulates Dreambox web application with the Internet Explorer browser.
Dreambox Microsoft Edge	This application simulates Dreambox web application with the Microsoft Edge browser.
eBanking Chrome to Apache	This application simulates a banking web application with the Google Chrome browser connecting to an Apache web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Firefox to IIS	This application simulates a banking web application with the Mozilla Firefox browser connecting to an IIS web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Internet Explorer to Nginx	This application simulates a banking web application with the Internet Explorer browser connecting to an Nginx web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
eBanking Microsoft Edge to Apache	This application simulates a banking web application with the Microsoft Edge browser connecting to an Apache web server. The user registers, logs into the website and performs common actions like viewing transactions, accounts and opening the contact page ended with logout.
EpixNow Chrome	This application simulates EpixNow web application with the Google Chrome browser.
EpixNow Firefox	This application simulates EpixNow web application with the Mozilla Firefox browser.

Application	Description
EpixNow Internet Explorer	This application simulates EpixNow web application with the Internet Explorer browser.
EpixNow Microsoft Edge	This application simulates EpixNow web application with the Microsoft Edge browser.
eShop Chrome to Apache	This application simulates an online shop web application with the Google Chrome browser connecting to an Apache web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Firefox to IIS	This application simulates an online shop web application with the Mozilla Firefox browser connecting to an IIS web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Internet Explorer to Nginx	This application simulates an online shop web application with the Internet Explorer browser connecting to an Nginx web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
eShop Microsoft Edge to Apache	This application simulates an online shop web application with the Microsoft Edge browser connecting to an Apache web server. The user searches for a product, views information about it, logs in, adds a product to the cart, deletes it from the cart and then logs out.
Facebook Audio Chrome	This application simulates Facebook Audio web application with the Google Chrome browser.
Facebook Audio Firefox	This application simulates Facebook Audio web application with the Mozilla Firefox browser.
Facebook Audio Internet Explorer	This application simulates Facebook Audio web application with the Internet Explorer browser.
Facebook Audio Microsoft Edge	This application simulates Facebook Audio web application with the Microsoft Edge browser.
Facebook Chrome	This application simulates Facebook web application with the Google Chrome browser.
Facebook Firefox	This application simulates Facebook web application with the Mozilla Firefox browser.
Facebook Internet Explorer	This application simulates Facebook web application with the Internet Explorer browser.
Facebook Microsoft Edge	This application simulates Facebook web application with the Microsoft Edge browser.

Application	Description
FacebookLive Chrome	This application simulates FacebookLive web application with the Google Chrome browser.
FacebookLive Firefox	This application simulates FacebookLive web application with the Mozilla Firefox browser.
FacebookLive Internet Explorer	This application simulates FacebookLive web application with the Internet Explorer browser.
FacebookLive Microsoft Edge	This application simulates FacebookLive web application with the Microsoft Edge browser.
Gab Chrome	This application simulates Gab web application with the Google Chrome browser.
Gab Firefox	This application simulates Gab web application with the Mozilla Firefox browser.
Gab Internet Explorer	This application simulates Gab web application with the Internet Explorer browser.
Gab Microsoft Edge	This application simulates Gab web application with the Microsoft Edge browser.
Gaode Maps Chrome	This application simulates Gaode Maps web application with the Google Chrome browser.
Gaode Maps Firefox	This application simulates Gaode Maps web application with the Mozilla Firefox browser.
Gaode Maps Internet Explorer	This application simulates Gaode Maps web application with the Internet Explorer browser.
Gaode Maps Microsoft Edge	This application simulates Gaode Maps web application with the Microsoft Edge browser.
Google Classroom Chrome	This application simulates Google Classroom web application with the Chrome browser.
Google Classroom Firefox	This application simulates Google Classroom web application with the Firefox browser.
Google Classroom Internet Explorer	This application simulates Google Classroom web application with the Internet Explorer browser.
Google Classroom Microsoft Edge	This application simulates Google Classroom web application with the Microsoft Edge browser.
Google Drive Chrome	This application simulates Google Drive web application with the Google Chrome browser.

Application	Description
Google Drive Firefox	This application simulates Google Drive web application with the Mozilla Firefox browser.
Google Drive Internet Explorer	This application simulates Google Drive web application with the Internet Explorer browser.
Google Drive Microsoft Edge	This application simulates Google Drive web application with the Microsoft Edge browser.
Google Sheets Chrome	This application simulates Google Sheets web application with the Chrome browser.
Google Sheets Firefox	This application simulates Google Sheets web application with the Firefox browser.
Google Sheets Internet Explorer	This application simulates Google Sheets web application with the Internet Explorer browser.
Google Sheets Microsoft Edge	This application simulates Google Sheets web application with the Microsoft Edge browser.
Google Slides Chrome	This application simulates Google Slides web application with the Chrome browser.
Google Slides Firefox	This application simulates Google Slides web application with the Firefox browser.
Google Slides Internet Explorer	This application simulates Google Slides web application with the Internet Explorer browser.
Google Slides Microsoft Edge	This application simulates Google Slides web application with the Microsoft Edge browser.
GoogleHangouts Chrome	This application simulates GoogleHangouts web application with the Chrome browser.
GoogleHangouts Firefox	This application simulates GoogleHangouts web application with the Firefox browser.
GoogleHangouts Internet Explorer	This application simulates GoogleHangouts web application with the Internet Explorer browser.
GoogleHangouts Microsoft Edge	This application simulates GoogleHangouts web application with the Microsoft Edge browser.
GooglePhotos Chrome	This application simulates GooglePhotos web application with the Chrome browser.
GooglePhotos Firefox	This application simulates GooglePhotos web application with the Firefox browser.

Application	Description
GooglePhotos Internet Explorer	This application simulates GooglePhotos web application with the Internet Explorer browser.
GooglePhotos Microsoft Edge	This application simulates GooglePhotos web application with the Microsoft Edge browser.
HTTP App	This application simulates a generic HTTP application.
Jingdong Chrome	This application simulates Jingdong web application with the Google Chrome browser.
Jingdong Firefox	This application simulates Jingdong web application with the Mozilla Firefox browser.
Jingdong Internet Explorer	This application simulates Jingdong web application with the Internet Explorer browser.
Jingdong Microsoft Edge	This application simulates Jingdong web application with the Microsoft Edge browser.
Jira Chrome	This application simulates Jira web application with the Chrome browser.
Jira Firefox	This application simulates Jira web application with the Firefox browser.
Jira Internet Explorer	This application simulates Jira web application with the Internet Explorer browser.
Jira Microsoft Edge	This application simulates Jira web application with the Microsoft Edge browser.
League of Legends Chrome	This application simulates League of Legends web application with the Google Chrome browser.
League of Legends Firefox	This application simulates League of Legends web application with the Mozilla Firefox browser.
League of Legends Internet Explorer	This application simulates League of Legends web application with the Internet Explorer browser.
League of Legends Microsoft Edge	This application simulates League of Legends web application with the Microsoft Edge browser.
Mail.ru Chrome	This application simulates Mail.ru web application with the Chrome browser.
Mail.ru Firefox	This application simulates Mail.ru web application with the Firefox browser.
Mail.ru Internet Explorer	This application simulates Mail.ru web application with the Internet Explorer browser.
Mail.ru Microsoft Edge	This application simulates Mail.ru web application with the Microsoft Edge browser.

Application	Description
Meraki Chrome	This application simulates Meraki web application with the Google Chrome browser.
Meraki Firefox	This application simulates Meraki web application with the Mozilla Firefox browser.
Meraki Internet Explorer	This application simulates Meraki web application with the Internet Explorer browser.
Meraki Microsoft Edge	This application simulates Meraki web application with the Microsoft Edge browser.
Mewe Chrome	This application simulates Mewe web application with the Google Chrome browser.
Mewe Firefox	This application simulates Mewe web application with the Mozilla Firefox browser.
Mewe Internet Explorer	This application simulates Mewe web application with the Internet Explorer browser.
Mewe Microsoft Edge	This application simulates Mewe web application with the Microsoft Edge browser.
MongoDB	This application simulates the MongoDB, a cross-platform document-oriented database.
Netease Music Chrome	This application simulates Netease Music web application with the Google Chrome browser.
Netease Music Firefox	This application simulates Netease Music web application with the Mozilla Firefox browser.
Netease Music Internet Explorer	This application simulates Netease Music web application with the Internet Explorer browser.
Netease Music Microsoft Edge	This application simulates Netease Music web application with the Microsoft Edge browser.
Office 365 Outlook People Chrome	This application simulates Office 365 Outlook People web application with the Chrome browser.
Office 365 Outlook People Firefox	This application simulates Office 365 Outlook People web application with the Firefox browser.
Office 365 Outlook People Internet Explorer	This application simulates Office 365 Outlook People web application with the Internet Explorer browser.
Office 365 Outlook	This application simulates Office 365 Outlook People web application with the

Application	Description
People Microsoft Edge	Microsoft Edge browser.
Office365 Excel Chrome	This application simulates Office365 Excel web application with the Google Chrome browser.
Office365 Excel Firefox	This application simulates Office365 Excel web application with the Mozilla Firefox browser.
Office365 Excel Internet Explorer	This application simulates Office365 Excel web application with the Internet Explorer browser.
Office365 Excel Microsoft Edge	This application simulates Office365 Excel web application with the Microsoft Edge browser.
Office365 OneDrive Chrome	This application simulates Office365 OneDrive web application with the Google Chrome browser.
Office365 OneDrive Firefox	This application simulates Office365 OneDrive web application with the Mozilla Firefox browser.
Office365 OneDrive Internet Explorer	This application simulates Office365 OneDrive web application with the Internet Explorer browser.
Office365 OneDrive Microsoft Edge	This application simulates Office365 OneDrive web application with the Microsoft Edge browser.
Office365 Outlook Chrome	This application simulates Office365 Outlook web application with the Google Chrome browser.
Office365 Outlook Firefox	This application simulates Office365 Outlook web application with the Mozilla Firefox browser.
Office365 Outlook Internet Explorer	This application simulates Office365 Outlook web application with the Internet Explorer browser.
Office365 Outlook Microsoft Edge	This application simulates Office365 Outlook web application with the Microsoft Edge browser.
OK.ru Chrome	This application simulates OK.ru web application with the Chrome browser.
OK.ru Firefox	This application simulates OK.ru web application with the Firefox browser.
OK.ru Internet Explorer	This application simulates OK.ru web application with the Internet Explorer browser.
OK.ru Microsoft Edge	This application simulates OK.ru web application with the Microsoft Edge browser.

Application	Description
Portal Chrome to Apache	This application simulates a portal web application with the Google Chrome browser connecting to an Apache web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Firefox to IIS	This application simulates a portal web application with the Mozilla Firefox browser connecting to an IIS web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Internet Explorer to Nginx	This application simulates a portal web application with the Internet Explorer browser connecting to an Nginx web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Portal Microsoft Edge to Apache	This application simulates a portal web application with the Microsoft Edge browser connecting to an Apache web server. The user logs into the website and performs common actions such as search and upload image before logs out.
Reddit Chrome	This application simulates Reddit web application with the Google Chrome browser.
Reddit Firefox	This application simulates Reddit web application with the Mozilla Firefox browser.
Reddit Internet Explorer	This application simulates Reddit web application with the Internet Explorer browser.
Reddit Microsoft Edge	This application simulates Reddit web application with the Microsoft Edge browser.
Salesforce Chrome	This application simulates Salesforce web application with the Chrome browser.
Salesforce Firefox	This application simulates Salesforce web application with the Firefox browser.
Salesforce Internet Explorer	This application simulates Salesforce web application with the Internet Explorer browser.
Salesforce Microsoft Edge	This application simulates Salesforce web application with the Microsoft Edge browser.
Service-Now Chrome	This application simulates Service-Now web application with the Google Chrome browser.
Service-Now Firefox	This application simulates Service-Now web application with the Mozilla Firefox browser.
Service-Now	This application simulates Service-Now web application with the Internet

Application	Description
Internet Explorer	Explorer browser.
Service-Now Microsoft Edge	This application simulates Service-Now web application with the Microsoft Edge browser.
Skype 8 Chrome	This application simulates Skype 8 web application with the Chrome browser.
Skype 8 Firefox	This application simulates Skype 8 web application with the Firefox browser.
Skype 8 Internet Explorer	This application simulates Skype 8 web application with the Internet Explorer browser.
Skype 8 Microsoft Edge	This application simulates Skype 8 web application with the Microsoft Edge browser.
Skype Chrome	This application simulates Skype web application with the Chrome browser.
Skype Firefox	This application simulates Skype web application with the Firefox browser.
Skype Internet Explorer	This application simulates Skype web application with the Internet Explorer browser.
Skype Microsoft Edge	This application simulates Skype web application with the Microsoft Edge browser.
SMTP	Emulates an SMTP Email session.
Social Network Chrome to Apache	This application simulates a social network web application with Google Chrome browser connecting to an Apache web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Firefox to IIS	This application simulates a social network web application with Mozilla Firefox browser connecting to an IIS web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Internet Explorer to Nginx	This application simulates a social network web application with Internet Explorer browser connecting to an Nginx web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Social Network Microsoft Edge to Apache	This application simulates a social network web application with Microsoft Edge browser connecting to an Apache web server. The user logs into the website, performs common actions such as view profile, like post, unlike post, create a post, comment to a post and then logs out.
Splunk Chrome	This application simulates Splunk web application with the Google Chrome browser.

Application	Description
Splunk Firefox	This application simulates Splunk web application with the Mozilla Firefox browser.
Splunk Internet Explorer	This application simulates Splunk web application with the Internet Explorer browser.
Splunk Microsoft Edge	This application simulates Splunk web application with the Microsoft Edge browser.
Tubi Chrome	This application simulates Tubi web application with the Chrome browser.
Tubi Firefox	This application simulates Tubi web application with the Firefox browser.
TWC Firefox	This application simulates TWC web application with the Firefox browser.
TWC Internet Explorer	This application simulates TWC web application with the Internet Explorer browser.
TWC Microsoft Edge	This application simulates TWC web application with the Microsoft Edge browser.
Video Platform Chrome to Apache	This application simulates a video platform web application with Google Chrome browser connecting to an Apache web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Firefox to IIS	This application simulates a video platform web application with Mozilla Firefox browser connecting to an IIS web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Internet Explorer to Nginx	This application simulates a video platform web application with Internet Explorer browser connecting to an Nginx web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
Video Platform Microsoft Edge to Apache	This application simulates a video platform web application with Microsoft Edge browser connecting to an Apache web server. The user logs into the website, performs common actions such as search video, download video, upload video, delete video, like video, unlike video and then logs out.
VKontakte Chrome	This application simulates VKontakte web application with the Chrome browser.
VKontakte Firefox	This application simulates VKontakte web application with the Firefox browser.
VKontakte Internet Explorer	This application simulates VKontakte web application with the Internet Explorer browser.

Application	Description
Vkontakte Microsoft Edge	This application simulates VKontakte web application with the Microsoft Edge browser.
Yammer Chrome	This application simulates Yammer web application with the Google Chrome browser.
Yammer Firefox	This application simulates Yammer web application with the Mozilla Firefox browser.
Yammer Internet Explorer	This application simulates Yammer web application with the Internet Explorer browser.
Yammer Microsoft Edge	This application simulates Yammer web application with the Microsoft Edge browser.
YYLive Chrome	This application simulates YYLive web application with the Google Chrome browser.
YYLive Firefox	This application simulates YYLive web application with the Mozilla Firefox browser.
YYLive Internet Explorer	This application simulates YYLive web application with the Internet Explorer browser.
YYLive Microsoft Edge	This application simulates YYLive web application with the Microsoft Edge browser.

APPENDIX C

Application Actions

The following table lists the application actions and action parameters available in LoadCore.

Application Action	Action Parameters	Parameter Description
<i>Adobe Reader Updates</i>		
Check For Updates	Current Version	Displays the current version.
	Update Version	Displays the update version.
Download Updates	Update Version	Displays the current version.
<i>ADP</i>		
Load Main Paige	N/A	N/A
Load Login Information Page	N/A	N/A
Load Employee Login Page	N/A	N/A
<i>Airbnb</i>		
Load First Page	City	Set the city name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
Specify Search Criteria	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Second selected rental	Set the second selected rental name.

Application Action	Action Parameters	Parameter Description
Select a Rental	Main rental photo	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Main rental photo (low resolution)	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo of host	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 2 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 3 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 4 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 5 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Airbnb host name	Set the airbnb host name.
	Reviewer	Set the reviewer name.
	Second reviewer	Set the second reviewer name.
	Third reviewer	Set the third reviewer name.
View Rental Photos	Thumbnail photo of host	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Thumbnail photo of first reviewer	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Thumbnail photo of third reviewer	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.

Application Action	Action Parameters	Parameter Description
	Checkout Date	Set the check-out date.
View More Amenities	City	Set the city name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
View Hot Profile	Thumbnail photo of first reviewer	
View Second Property	Photo 3 of rental	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.
	Checkout Date	Set the check-out date.
	Selected rental name	Set the selected rental name.
	Airbnb host name	Set the airbnb host name.
	Reviewer	Set the reviewer name.
	Second reviewer	Set the second reviewer name.
	Third reviewer	Set the third reviewer name.
	Second selected rental	Set the second selected rental name.
	Photo 1 of rental	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
	Photo 4 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Photo 5 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	City	Set the city name.
	Second selected rental	Set the second selected rental name.
View the Calendar	N/A	N/A
<i>appointy</i>		
Load Login Page	User name	Set the user name.
Login	User name	Set the user name.
	Password	Provide the password
	Profession	Set the profession.
	City	Set the city name.
	State/Province	Set the state/province name.
	Staff member 1	Set the name of the first staff member.
	Staff member 2	Set the name of the second staff member.
	Customer 1 first name	Set the first name of Customer 1.
	Customer 1 last name	Set the last name of Customer 1.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.

Application Action	Action Parameters	Parameter Description
Book New Customer	User name	Set the user name.
	Full manager name	Set the manager name.
	City	Set the city name.
	State/Province	Set the state/province name.
	Service	Set the service name.
	Staff member 1	Set the name of the first staff member.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.
View New Users Pulldown	User name	Set the user name.
View New Appointments Pulldown	User name	Set the user name.
Select Dashboard Tab	User name	Set the user name.
	Profession	Set the profession.
Select Reports Tab	User name	Set the user name.
View Week Calendar	User name	Set the user name.
View Customers Tab	User name	Set the user name.
	City	Set the city name.
	Customer 1 first name	Set the first name of Customer 1.
	Customer 1 last name	Set the last name of Customer 1.
	Customer 2 first name	Set the first name of Customer 2.
	Customer 2 last name	Set the last name of Customer 2.

Application Action	Action Parameters	Parameter Description
Logout	User name	Set the user name.
<i>AWS Console</i>		
Load AWS Page	N/A	N/A
Load AWS Management Console	Region name	Set the region name.
Sign In	User email	Provide the user email.
	Password	Provide the password.
	User name	Set the user name.
	Region name	Set the region name.
Check Account Info	User email	Provide the user email.
	Region name	Set the region name.
Check Account Billing	User email	Provide the user email.
	Region name	Set the region name.
Check Credentials	Region name	Set the region name.
	Existing keyID 1	Provide the existing keyID 1.
	Existing keyID 2	Provide the existing keyID 2.
Create New Access Key	New KeyID	Set the new keyID.
Download Key file	New KeyID	Set the new keyID.
	Key file name	Set the key file name.
Delete Key	Existing keyID 1	Provide the existing keyID 1.
Sign Out	User email	Provide the user email.
	Region name	Set the region name.
<i>AWS S3</i>		

Application Action	Action Parameters	Parameter Description
Check Buckets Names	User email	Provide the user email.
	Region name	Set the region name.
	KeyID	Provide the keyID.
Create Buckets	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
Upload File	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket bame	Set the source bucket name.
	Local file name for upload	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
List Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Source file name	Set the source file name.
Copy Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
	Source file name	Set the source file name.

Application Action	Action Parameters	Parameter Description
Verify Copied Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Destination bucket name	Set the destination bucket name.
Download Files	Region name	Set the region name.
	KeyID	Set the keyID.
	Source bucket name	Set the source bucket name.
	Source file name	Set the source file name.
Delete Files and Buckest	User email	Provide the user email.
	Region name	Set the region name.
	KeyID	Provide the keyID.
	Source bucket name	Set the source bucket name.
	Destination bucket name	Set the destination bucket name.
	Source file name	Set the source file name.
<i>Baidu</i>		
Access Baidu News	N/A	N/A
Access Baidu Maps	N/A	N/A
Access Baidu Pictures	N/A	N/A
Load Maine Paige	N/A	N/A
Search String	Search query	Provide the search criteria.
Search Image	Baidu search image file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
Access Baidu Passport	N/A	N/A
<i>Baidu Maps</i>		
Load Web Page	N/A	N/A
Search a Place	Query string	Provide the search criteria.
Finding a route	Query string	Provide the search criteria.
	Source location	Set the search location.
	Destination location	Set the destination location.
<i>Bilibili</i>		
Open Bilibili Website	N/A	N/A
Login	Username	Provide the username.
	Password	Provide the password.
Search Video	Video name	Provide the video name.
Watch Video	N/A	N/A
Upload Video	Uploaded video title	Set the title for the uploaded video.
	Uploaded video file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout	N/A	N/A
<i>Cisco Spark</i>		
Start the Application	N/A	N/A
Click Get Started	N/A	N/A
Click Next	User email address	Provide the user's email address.
Click SignIn	The contact's	Provide the contact's first/last name.

Application Action	Action Parameters	Parameter Description
Sign In	first/last name	
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
	Password	Provide the password.
	User's first/last name	Provide the user's first/last name
Create a Team	User email address	Provide the user's email address.
Add Contact	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Send Message	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Send File	User email address	Provide the user's email address.
	User's first/last name	Provide the user's first/last name
Initiate a Call	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.

Application Action	Action Parameters	Parameter Description
Hang Up Call	The contact's first/last name	Provide the contact's first/last name.
	User email address	Provide the user's email address.
	The contact's email address	Provide the contact's email address.
Exit	N/A	N/A
<i>Commvault</i>		
Get Login Page	N/A	N/A
Login	User email	Provide the user's email address.
	Password	Provide the password.
View Drive	N/A	N/A
Create Folder	Created folder name	Set the name of the created folder.
Rename Folder	Folder name	Set the folder's new name.
Move File	Folder name	Provide the folder name.
Navigate To Folder	Folder name	Provide the folder name.
Upload File	Uploaded file name	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Download File	Downloaded file name	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Get Public Link	Folder ID	Provide the folder ID.
Move File To Trash	N/A	N/A
View Trash	N/A	N/A

Application Action	Action Parameters	Parameter Description
Restore File From Trash	Folder name	Provide the folder name.
Empty Trash	N/A	N/A
View Public Links	N/A	N/A
Deelte Public Link	Folder ID	Provide the folder ID.
Log Out	N/A	N/A
<i>Crawling Wikipedia (Chinese)</i>		
Crawl Link 1	Root URI	Set the root URI.
Crawl Link 2	Root URI	Set the root URI.
Crawl Link 3	Root URI	Set the root URI.
Crawl Link 4	Root URI	Set the root URI.
<i>DocuSign</i>		
Load Front Page	N/A	N/A
<i>Dreambox</i>		
Login	Login email address	Provide the login email address.
	Password	Provide the password.
Open Dashboard	N/A	N/A
Check Activity Status	From date	Set the starting date.
	To date	Set the end date.
Add Assignment	Select a grade	Set a grade.
	Select a category	Set a category.
	Short description	provide a short description.
Set Dreambox Game	N/A	N/A
Pause Dreambox Game	N/A	N/A
Quit Dreambox	N/A	N/A

Application Action	Action Parameters	Parameter Description
Game		
Logout	N/A	N/A
<i>eBanking</i>		
Sign Up	SignUp username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	SignUp password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	SignUp confirm password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Login	Login username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
View Transactions	N/A	N/A
View Accounts	N/A	N/A
Get Contact Page	N/A	N/A
Logout	N/A	N/A
<i>EpixNow</i>		

Application Action	Action Parameters	Parameter Description
Open Login Page	N/A	N/A
Login	Email	Provide the login email address.
	Password	Provide the password.
Browse Movies	Search keyword	Provide the search criteria.
Search Movies	Search keyword	Provide the search criteria.
Play	Search keyword	Provide the search criteria.
Logout	N/A	N/A
<i>eShop</i>		
Search Product	Product name	Provide the product name.
View Product	Product ID	Provide the product ID.
Login	Login username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Add To Cart	N/A	N/A
Remove From Cart	N/A	N/A
Buy	Full name	Provide the full name.
	Address	Provide the address.
	Account number	Provide the account number.
Logout	N/A	N/A
<i>Facebook Audio</i>		
Open Home Page	N/A	N/A
Login	Encrypted	Provide the password.

Application Action	Action Parameters	Parameter Description
	password	
	Email	Provide the login email address.
Create Audio Room	N/A	N/A
Join Audio Room	N/A	N/A
Leave Audio Room	N/A	N/A
Logout	N/A	N/A
<i>Facebook</i>		
Get Homepage	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User first name	Provide the first name.
	User second name	Provide the second name.
Open Notifications	N/A	N/A
Search Person	Search string	Provide the search criteria.
Add Friend	Friend first name	Provide the friend's first name.
	Friend second name	Provide the friend's second name.
Send Message	Message body	Provide the message.
	Recipient first name	Provide the recipient's first name.
	Recipient second name	Provide the recipient's second name.

Application Action	Action Parameters	Parameter Description
Send Message With Attachment	Message body	Provide the message.
	Recipient first name	Provide the recipient's first name.
	Recipient second name	Provide the recipient's second name.
	Filename	Provide the file name
	Upload File	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Download Attachment	Download file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Go To Profile	N/A	N/A
Post In News Feed	Post Message	Provide the message.
	Post file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Comment Post	Comment message	Provide the post message.
	Post author	Provide the post's author.
Delete Comment	Post author	Provide the post's author.
Like Post	N/A	N/A
Unlike Post	N/A	N/A
Sign Out	N/A	N/A
<i>FacebookLive</i>		

Application Action	Action Parameters	Parameter Description
Sign In	C_user cookie2	Set the value.
	C_user cookie	Set the value.
	User email address	Provide the user email address.
	Password	Provide the password.
	User name	Provide the username.
	Friend 1 first name	Provide the first name.
Start Live Stream	C_user cookie	Set the value.
	User name	Provide the username.
	Friend 1 first name	Provide the first name.
	Friend 3 first name	Provide the first name.
	Video stream ID	Set the video stream ID.
Sign Out	C_user cookie	Set the value.
	User email address	Provide the user email address.
	User name	Provide the username.
	Video stream ID	Set the video stream ID.
<i>Gab</i>		
Open Home Page	N/A	N/A
Open Login Page	N/A	N/A
Login	Email	Provide the email address.
	Password	Provide the password.
Read News	N/A	N/A
Post News	Statut text	Provide the message.
Logout	N/A	N/A

Application Action	Action Parameters	Parameter Description
<i>Gaode Maps</i>		
Open Website	N/A	N/A
Search Location	Destination	Provide the destination.
Find Route	Destination	Provide the destination.
	Starting location	Provide the starting location.
	Transportation method	Provide the transportation method.
<i>Google Classroom</i>		
Load Homepage	N/A	N/A
Login	Username	Provide the username.
	User email	Provide the email address.
	User password	Provide the password.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
Create New Classroom	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Create New Post	Post text	Provide the text message.
Edit Post	Post text	Provide the text message.
Add Attachment to Post	Post attachment	Select an option:

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Post text	Provide the text message.
Load Classroom Tab	N/A	N/A
Create New Assignment	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Add Attachment to Assignment	Assignment document	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Assignment title	Provide the assignment title.
Load People Tab	N/A	N/A
Invite a Student	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.

Application Action	Action Parameters	Parameter Description
Student Load Homepage	Post attachment	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Student Add Submission	Submission document compressed	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Add Student Private Comment	Student private comment	Provide the comment.
Load Grades Tab	Assignment title	Provide the assignment title.

Application Action	Action Parameters	Parameter Description
View Submission	Submission document	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Submission document webp format	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Assignment title	Provide the assignment title.
	Student private comment	Provide the comment.
Add Professor Private Comment	Username	Provide the username.
	User email	Provide the email address.
	Student username	Provide the student's username.
	Student email	Provide the student's email address.
	Assignment title	Provide the assignment title.
	Student private comment	Provide the comment.
	Professor private comment	Provide the comment.
Grade Submission	Grade of the	Provide the grade value.

Application Action	Action Parameters	Parameter Description
	assignment	
Archive Classroom	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
	Post text	Provide the text message.
	Assignment title	Provide the assignment title.
Delete Classroom	Classroom name	Set the classroom name.
	Section name	Set the section name.
	Room name	Set the room name.
	Subject name	Set the subject name.
Logout	Username	Provide the username.
	User email	Provide the email address.
<i>Google Drive</i>		
Get Sigh In Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Create Folder	Folder name	Set the folder name.
Upload File	File name	Provide the file name.
	Upload file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Delete File	File name	Provide the file name.
Empty Bin	File name	Provide the file name.
	File content	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Create Text Document	Document content	Provide the document content.
	Document name	Provide the document name.
Create Presentation	Powerpoint content	Provide the content.
	Powerpoint name	Provide the name.
Create Spreadsheet	Spreadsheet content	Provide the content.
	Spreadsheet name	Provide the name.
Download File	File name	Provide the file name.
	Downloaded file	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Sign Out	N/A	N/A
<i>Google Sheets</i>		
Load Sigh In Page	N/A	N/A
Sign In	Username	Provide the username.
	Password	Provide the password.

Application Action	Action Parameters	Parameter Description
Create a New Sheet	N/A	N/A
Input Data	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Key text 1	Provide the key text.
	Value text 1	Provide the value text
	Key text 2	Provide the key text.
	Value text 2	Provide the value text
	Key text 3	Provide the key text.
	Value text 3	Provide the value text
Share the Sheet	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Receiver username	Provide the username of the receiver.
Complete sharing	Username	Provide the username.
	Sheet name	Provide the sheet name.
	Receiver username	Provide the username of the receiver.
	Sharing note	Provide the text for the sharing note.
Sign Out	Username	Provide the username.
<i>Google Slides</i>		
Load Sigh In Page	N/A	N/A
Sign In	Username	Provide the username.
	Password	Provide the password.
Start a New Presentation	Username	Provide the username.
Start a New Slide	N/A	N/A
Input Slide Text	Slide Name	Provide the value.

Application Action	Action Parameters	Parameter Description
Replace Image	Username	Provide the username.
	File attachment	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Name the Slide	Slide name	Provide the value.
Share the Slide	Username	Provide the username.
	Slide name	Provide the value.
	Receiver username	Provide the username of the receiver.
Send Sharing	Receiver username	Provide the username of the receiver.
Sign Out	Username	Provide the username.
<i>GoogleHangouts</i>		
Load First Page	N/A	N/A
Sign In	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Password	Provide the password.
	Other user's first/last name	Provide the other user's first/last name.
Start Chat	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
Send Text Message	First chat text message	Provide the text message.

Application Action	Action Parameters	Parameter Description
Receive Text Message	N/A	N/A
Send a File	User email address	Provide the user email address.
	Second chat text message	Provide the text message.
Receive Text Reply	User email address	Provide the user email address.
Send Image	N/A	N/A
Receive Image	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
	First chat text message	Provide the text message.
	Second chat text message	Provide the text message.
Make Phone Call	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Phone number	Provide the phone number.
Start Video Call	User's first/last name	Provide the user's first/last name.
	User email address	Provide the user email address.
	Other user's first/last name	Provide the other user's first/last name.
Logout	User's first/last name	Provide the user's first/last name.

Application Action	Action Parameters	Parameter Description
	User email address	Provide the user email address.
<i>GooglePhotos</i>		
Load Login Page	N/A	N/A
Login to Google	Password	Provide the password.
	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
View a Photo	User email address	Provide the user email address.
	Full user name	Provide the username.
View Next Photo	Full user name	Provide the username.
Return to Main Page	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
View Albums Page	Shared folder name	Provide the folder name.
Select an Album	User email address	Provide the user email address.
	Full user name	Provide the username.
	Shared folder name	Provide the folder name.
Upload a Photo	Uploaded Photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to

Application Action	Action Parameters	Parameter Description
		upload a file.
Return to Photos Page	N/A	N/A
Download a Photo	Full user name	Provide the username.
	Downloaded photo	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout of Google	User email address	Provide the user email address.
	Full user name	Provide the username.
<i>HTTP</i>		

Application Action	Action Parameters	Parameter Description
HTTP GET	Path	The value of the path requested.
	Query	The value of the query requested.
	Request headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Accept-Language • Sec-Fetch-User • Upgrade-Insecure-Requests • Sec-Fetch-Site <p>Use the Add button to add new options or the Delete to remove them.</p>
	Status code	The value of the response status code.
	Reason phrase	The value of the reason phrase.
	Response headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Cache-Control • Etag <p>Use the Add button to add new options or the Delete to remove them.</p>
	Response body	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file. • Dynamic payload - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
HTTP POST	URL	Provide the URL.
	Request headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Sec-Fetch-User • Upgrade-Insecure-Requests • Accept-Language • Sec-Fetch-Site <p>Use the Add button to add new options or the Delete to remove them.</p>
	Request body	<p>Select an option:</p> <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file. • Dynamic payload - select an option from the drop-down list or use the Upload button to upload a file.
	Status code	The value of the response status code.
	Reason phrase	The value of the reason phrase.
	Response headers	<p>The name-value options provided are:</p> <ul style="list-style-type: none"> • Etag • Cache-Control <p>Use the Add button to add new options or the Delete to remove them.</p>
	Response Body	Add a response message.
<i>Jingdong</i>		
Go To Jingdong	N/A	N/A
Login	Username	Provide the username.
Search For products	Search keyword	Provide the search criteria.
Check Products Information	N/A	N/A

Application Action	Action Parameters	Parameter Description
Checkout	Username	Provide the username.
	Product name	Provide the product name.
	Order ID	Provide the order ID.
Logout	N/A	N/A
<i>Jira</i>		
Load Login Page	Story name	Provide the story name.
Login	Login email address	Provide the login email address.
	Password	Provide the password.
Create Project	Login email address	Provide the login email address.
	Project name	Provide the project name.
Create Story	Project name	Provide the project name.
	Story name	Provide the story name.
Add Comments to Story	Story name	Provide the story name.
Mark The Story To Closed	Story name	Provide the story name.
Logout	Story name	Provide the story name.
<i>League of Legends</i>		
Login	User ID	Provide the user ID.
Start Game	User ID	Provide the user ID.
Attack	N/A	N/A
<i>Mail.ru</i>		
Login	Username	Provide the username.
	Password	Provide the password.

Application Action	Action Parameters	Parameter Description
Send Mail	Fullscreen	Provide the fullname.
	Recipient email address	Provide the recipient email address.
	Recipient email subject	Provide the email subject.
	Recipient email body	Provide the email body.
View Mail	Fullscreen	Provide the fullname.
	Message sender email	Provide the sender email.
	Message sender name	Provide the sender name.
	View message subject	Provide the message subject.
	View message body	Provide the message body.
Logout	N/A	N/A
<i>Meraki</i>		
Login	Dashboard email address	Provide the email address.
	Dashboard password	Provide the password.
Enroll Device	New device address	Provide the device address.
	Enrollment message	Provide an enrollment message.
Add Application	New device address	Provide the device address.
	New application search query	Provide the search criteria.
Add Profile	New device address	Provide the device address.

Application Action	Action Parameters	Parameter Description
	Test profile name	Provide the test profile name.
	Test profile description	Provide the test profile description.
	Backup file name	Provide the backup file name.
Push Updates	N/A	N/A
View Clients	New device address	Provide the device address.
View Map	New device address	Provide the device address.
View Logs	New device address	Provide the device address.
Download CSV	Dashboard email address	Provide the email address.
Send Command	Remote command line	Provide the remote command line,
View Summary	New device address	Provide the device address.
Add Geofence	Geofence name	Provide the geofence name.
	Area name	Provide the area name.
Add Policy	Policy name	Provide the policy name
Add owner	New device address	Provide the device address.
	Owner name	Provide the name.
	Owner username	Provide the username.
	Owner password	Provide the password.
	Owner email	Provide the email.
Logout	N/A	N/A
<i>Mewe</i>		
Open Login Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Login	Email	Provide the email address.
	Password	Provide the password.
Read News Feed	N/A	N/A
Post Status	Status message	Provide the message text.
Logout	N/A	N/A
<i>MongoDB</i>		
Insert	N/A	N/A
Update	N/A	N/A
Query	N/A	N/A
Get More	N/A	N/A
Delete	N/A	N/A
Kill Cursor	N/A	N/A
Diagnostic Messages	N/A	N/A
<i>Netease</i>		
Go to Netease Music	N/A	N/A
Login	N/A	N/A
Search Music	Artist ID	Provide the artist ID.
PlayMusic	Music file name 1	Provide the music file name.
	Music file name 2	Provide the music file name.
	Music file name 3	Provide the music file name.
	Music file name 4	Provide the music file name.
Add To Playlist	Artist ID	Provide the artist ID.
Recommend Music	Artist ID	Provide the artist ID.

Application Action	Action Parameters	Parameter Description
Watch Music Video	Artist ID	Provide the artist ID.
	Music video ID 1	Provide the music video ID.
	Music video ID 2	Provide the music video ID.
	Music video ID 3	Provide the music video ID.
	Music video ID 4	Provide the music video ID.
Logout	N/A	N/A
<i>Office 365 Outlook People</i>		
Get Sign In Page	N/A	N/A
Sign In	User name	Provide the user name.
	Password	Provide the password.
Create a New Contact	Contact first name	Provide the first name.
	Contact last name	Provide the last name.
	Contact email	Provide the email address.
Search for a Contact	Search people	Provide the search criteria.
Delete a Contact	Contact email	Provide the email address.
Sign Out	N/A	N/A
<i>Office365 Excel</i>		
Get Home Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.

Application Action	Action Parameters	Parameter Description
Get Excel Tab	N/A	N/A
Get Excel Workbook	Workbook name	Provide the workbook name.
Edit Workbook	Content	Provide the content.
Pin Workbook	Workbook name	Provide the workbook name.
Open Workbook In OneDrive	N/A	N/A
Sign Out	N/A	N/A
<i>Office365 OneDrive</i>		
Get Home Page	N/A	N/A
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Get OneDrive Tab	N/A	N/A
Delete File	File name	Provide the file name.
Upload File	File name	Provide the file name.
	Upload file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Create Folder	Folder name	Provide the folder name.
Create Excel Workbook	Workbook name	Provide the workbook name.
Create Word	Document name	Provide the document name.

Application Action	Action Parameters	Parameter Description
Document		
Create Powerpoint Presentation	Powerpoint name	Provide the powerpoint name.
Sign Out	N/A	N/A
<i>Office365 Outlook</i>		
Sign In	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
View Inbox	N/A	N/A
Send Message	Recipient	Provide the email address.
	Subject	Provide the email subject.
	Body	Provide the email body text.
Send Message With Attachment	Recipient	Provide the email address.
	Subject	Provide the email subject.
	Body	Provide the email body text.
	Attachment	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
	Attachment filename	Provide the file name.
Open Message	N/A	N/A
Delete Message	N/A	N/A

Application Action	Action Parameters	Parameter Description
Navigate To Calendar Panel	N/A	N/A
Create A New Event	Event date	Set the event date.
	Event start time	Set the start time.
	Event end time	Set the end time
	Event name	Set the event name.
Delete An Event	Event date	Set the event date.
	Event start time	Set the start time.
	Event end time	Set the end time
	Event name	Set the event name.
Navigate to People Panel	N/A	N/A
Create a New Contact	Contact email	Provide the address email.
	First name	Provide the first name.
	Second name	Provide the second name.
	Phone number	Provide the phone number.
Search For A Contact	Search string	Provide the search criteria.
Delete A Contact	Contact email	Provide the address email.
	First name	Provide the first name.
	Second name	Provide the second name.
	Phone number	Provide the phone number.
Navigate To Task Panel	N/A	N/A
Create New Task	Task title	Provide the task tile.
Mark Task Completed	Task title	Provide the task tile.
Delete Task	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign Out	N/A	N/A
<i>OK.ru</i>		
Login	Username	Provide the user name.
	Password	Provide the password.
View Feed	N/A	N/A
Post Message	Message	Provide the message text.
Logout	N/A	N/A
<i>Portal</i>		
Login	User email	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	User password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Search Image	Search query	Provide the search criteria.
Upload Image	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Logout	N/A	N/A
<i>Reddit</i>		
Load Main Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Sign In	Username	Provide the user name.
	Account password	Provide the password.
Access Post	N/A	N/A
Create Comment	Comment content	Provide content for the comment.
Delete Comment	N/A	N/A
Search Posts	Query string	Provide the search criteria.
Subscribe to Subreddit	Subreddit	Provide the subreddit.
Access Gifts Page	Subreddit	Provide the subreddit.
Load Profile	Username	Provide the user name.
Access Settings	N/A	N/A
Access Messages	N/A	N/A
Sign Out	N/A	N/A
<i>Salesforce</i>		
Load Login Page	User name	Provide the user name.
Login	User name	Provide the user name.
	Login email address	Provide the login email address.
	Password	Provide the password.
Select Top Deal	User name	Provide the user name.
	Login email address	Provide the login email address.
Update Call Log	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Opportunities Tab	Login email address	Provide the login email address.

Application Action	Action Parameters	Parameter Description
Select An Opportunity	User name	Provide the user name.
	Login email address	Provide the login email address.
Edit Amount	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Notes Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Edit a Note	User name	Provide the user name.
	Login email address	Provide the login email address.
Select Dashboards Tab	User name	Provide the user name.
	Login email address	Provide the login email address.
Open 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 file.

Application Action	Action Parameters	Parameter Description
		file.
News feed	N/A	N/A
View Profile	Member ID	Provide the member ID.
Like Post	N/A	N/A
Unlike Post	N/A	N/A
Create Post	Post content	Provide the content.
Comment To Post	Original post ID	Provide the post ID.
	Comment content	Provide the content.
Logout	N/A	N/A
<i>Splunk</i>		
Load Login Page	N/A	N/A
Login	Username	Provide the user name.
	Password	Provide the password.
Upload Log	Description	Provide a description.
	Index	Provide the index.
	Log File	Select an option: <ul style="list-style-type: none"> • Synthetic data (bytes) and set the value. • Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Search Log	Index	Provide the index.
Logout	Username	Provide the user name.
<i>Tubi</i>		
Open Tubi Page	N/A	N/A

Application Action	Action Parameters	Parameter Description
Login	Email address	Provide the email address.
	Password	Provide the password.
	User ID	Provide the user ID.
	User name	Provide the user name.
Browse Tubi	Genre	Provide the genre.
Select Movie	Genre	Provide the genre.
	Movie name	Provide the movie name.
	Movie duration	Provide the movie duration.
	Movie description	Provide the movie description.
	Movie director	Provide the movie director.
	Movie release year	Provide the release year.
	Movie actor 1	Provide the movie actor.
	Movie actor 2	Provide the movie actor.
	Movie content ID	Provide the movie content ID.
	Recommended movie name	Provide the recommended movie name.
Play Video	Movie content ID	Provide the movie content ID.
Pause Video	Movie content ID	Provide the movie content ID.
Select Recommended Movie	Genre	Provide the genre.
	Recommended movie name	Provide the recommended movie name.
	Recommended movie duration	Provide the recommended movie duration.
Logout	N/A	N/A
<i>TWC</i>		
Open The Weather Channel App	N/A	N/A

Application Action	Action Parameters	Parameter Description
View 48 Hours Details	N/A	N/A
View 15 Days Details	N/A	N/A
Swipe to Bottom of Main Page	N/A	N/A
<i>Video Platform</i>		
Login	Login username	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
	Login password	Select an option: <ul style="list-style-type: none">• User input and provide the value.• Playlist file - select an option from the drop-down list or use the Upload button to upload a file.
Search Video	Video name	Provide the video name.
Download video	Downloaded file name	Provide the file name.
	Downloaded file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Upload Video	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none">• Synthetic data (bytes) and set the value.• Payload profile - select an option from the drop-down list or use the Upload button to upload a file.
Delete Video	N/A	N/A

Application Action	Action Parameters	Parameter Description
Like Video	N/A	N/A
Unlike Video	N/A	N/A
Logout	N/A	N/A
VKontakte		
Load Login page	N/A	N/A
Login	Username	Provide the user name.
	Password	Provide the password.
View Feed	View feed message	Provide the message.
Post Message	Post message	Provide the message.
Logout	N/A	N/A
Yammer		
Select First Group	User email address	Provide the email address.
	User name	Provide the user name.
Select Second Group	User email address	Provide the email address.
Select Third Group	User email address	Provide the email address.
Like an Entry	User email address	Provide the email address.
Reply to a Post	User email address	Provide the email address.
	User name	Provide the user name.
Post New Message	User email address	Provide the email address.
	User name	Provide the user name.
Select Another Group	User email address	Provide the email address.

Application Action	Action Parameters	Parameter Description
<i>YYLive</i>		
Load Home Page	N/A	N/A
Select Category	Category	Provide the category.
Play Video	Video ID	Provide the Video ID.

Index

5

5G-EIR, configuration settings 238

A

Agent Assignment window 65

AMF, configuration settings 105

application traffic generator 122, 281, 290, 293, 456, 461, 467, 500

AUSF, configuration settings 99, 345

B

bidirectional UDP traffic flow 124, 283, 457, 502

C

create/delete PDU session, secondary objective 277

create/delete QoS Flows, secondary objective 275, 448

customer assistance 3

D

discovery, NRF 304

DN, configuration settings 497

DNN settings

 Full Core tests 85

 SBA tests 317

E

enter/exit idle, secondary objective 274, 447

EPS fallback 173

F

Full Core tests

 configuration settings 71

 global settings 78

network slicing 260

objectives 264

H

handover, secondary objective 445

I

IPFilterRule 430

M

middleware VM, upgrade 51

modify QoS Flows, secondary objective 449

N

Nnrf_NFDiscovery 304

NRF discovery 304

NRF, configuration settings 141, 337

O

objectives

 Full core tests 264

 SBA tests 394

 UPF Isolation tests 440

P

packet filters

 for SDF 430

 packet filter list configuration 96, 324

Paging, secondary objective 273, 446

passthrough testing 509

PCF, configuration settings 157, 351

product support 3

Q

QoS flows, settings 92

R

RAN, configuration settings 166, 483

S

SBA tests

 configuration settings 307

 global settings 312

 network slicing 388

 objectives 394

SCP configuration settings 144, 341

SGW-U, configuration settings 226

SMF, configuration settings 195, 478

SMS, secondary objective 278

stateless UDP traffic generator 129, 280, 507

support services 3

T

TCP connection settings 314

technical support 3

traffic agents 65

traffic generators 121, 279, 453, 500

U

UDM, configuration settings 209, 359

UDP stateless, traffic generator 129, 280, 507

UDR, configuration settings 218, 356

UE configuration settings

 Full Core tests 242

 SBA tests 378

 UPF Isolation tests 432

UPF Isolation tests

 configuration settings 421

 global settings 424

 objectives 440

UPF, configuration settings 226, 487

URRs 431

