

LoadCore

Release 4.1

User Guide

Notices

Copyright Notice

© Keysight Technologies 2019–2023

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

Warranty

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

Technology Licenses

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

U.S. Government Rights

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

Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at <http://www.keysight.com/find/sweula>. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of 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	22
Chapter 2 Licensing Requirements	23
Chapter 3 Web Interface	24
Recommended Browsers	25
Access LoadCore Web UI	25
LoadCore Web UI	25
Chapter 4 How Do I...	28
Configure and run a test	29
Create test scenarios	34
Work with saved test configurations	34
Licensed Test Configs	40
Upgrade the MiddleWare VM	57
Configure Dashboard general settings	58
Configure LoadCore with LDAP/AD	59
Reset Password for Regular Users	63
Debug	65
View Notifications and Test Events	65
View Statistics	66
Manage Test Results	67
Collect Diagnostics	67
Chapter 5 License Manager	69
Chapter 6 Traffic agents assignment and management	71
Chapter 7 Full Core tests: configuration settings	77
Global Settings	85
Global Settings panel	87

Node Start/Stop Rates	87
DNS Settings	88
Advanced Settings	88
DNNs panel	93
DNN configuration settings	94
Session AMBR configuration settings	97
ePCO configuration settings	98
Traffic Control Settings configuration	98
Impairment	99
QoS Flows panel	100
QoS Flow configuration settings	101
QoS Flow Max Packet Loss Rate settings	103
QoS Flow ARP configuration settings	104
QoS Flow MBR configuration settings	104
QoS Flow GBR configuration settings	105
Milenage	105
Customer Parameters	106
CA Certificates	106
UE configuration settings	107
UE Ranges panel	108
UE Range panel	109
Range Settings	111
UE Identification settings	112
UE Security settings	112
UE Settings settings	116
UE Shared Data IDs	120
UE Subscribed AMBR settings	120
Service Area Restriction settings	120
Forbidden Areas	122
DNNs Config	123
Notifications	126

SMS Configuration	126
Equipment Status	127
Converged Charging	128
Spending Limit Control	129
Internal Group IDs	131
Network Slicing settings	133
UE NSSAI settings	134
UDM Default NSSAI settings	135
UDM SNSSAI Mappings	135
UDR SNSSAI Settings	136
Objectives	137
Control Plane Objective	138
About primary objectives	139
Primary Control Plane Objective	141
Secondary Control Plane Objective	143
User Plane Objectives	153
Stateless UDP Traffic	154
Data Traffic	155
Voice Traffic	159
Video OTT Traffic	173
DNS Client Traffic	176
ICMP Client	179
Ping Traffic	180
Capture Replay	181
Predefined Applications Traffic	183
AMF configuration settings	194
AMF Ranges panel	195
AMF Range settings	196
AMF node settings	197
AMF N2 interface settings	200
AMF Namf interface settings	201

AMF N26 Interface Settings	202
AMF remote SBA nodes	203
AUSF configuration settings	210
AUSF Ranges panel	211
AUSF Range panel	211
AUSF node settings	212
AUSF Nausf interface settings	213
AUSF Remote SBA Nodes	214
CHF configuration settings	217
CHF Ranges panel	217
CHF Range settings	218
CHF node settings	219
CHF Nchf interface settings	219
CHF remote SBA nodes	220
DN configuration settings	222
DN Ranges panel	223
DN Range panel	223
DN N6 interface settings	224
DN routes settings	225
DN User Plane	226
DN Stateless UDP Traffic	227
DN Data Traffic	228
DN Voice Traffic	231
DN Video OTT Traffic	241
DN DNS Server Traffic	244
DN Predefined Applications Traffic	246
DN Capture Replay	247
DNS Server configuration settings	250
DNS Server Ranges panel	250
DNS Server Range panel	250
DNS Server Ndnnserver interface settings	251

DNS Server Traffic Flow settings	252
IMS configuration settings	255
CSCF Range panel	255
CSCF N6 interface settings	256
CSCF Rx interface settings	257
CSCF UE routes settings	258
Media Function Range panel	259
MME configuration settings	261
MME Ranges panel	262
MME Range panel	263
MME node settings	264
MME S11 Interface Settings	265
MME N26 Interface Settings	266
MME S1 Interface Settings	267
MME S6a Interface Settings	269
MME Diameter settings	270
NEF configuration settings	271
NEF Ranges panel	271
NEF Range panel	271
NEF Nnef interface settings	272
NEF Remote SBA Nodes	273
NRF configuration settings	276
NRF Ranges panel	277
NRF Range panel	277
NRF node settings	278
NRF Nnrf interface settings	279
NRF Remote SBA Nodes	280
NSSF configuration settings	282
NSSF Ranges panel	283
NSSF Range panel	283
NSSF node settings	284

Nnssf Interface Settings	285
Remote SBA nodes	286
NSF Restricted NSSAIs	287
NSF Network Slices	288
NSF Configured NSSAI	289
PCF/PCRF configuration settings	290
PCF/PCRF Ranges panel	291
PCF Range panel	292
PCF node settings	293
PCRF node settings	294
PCF service area restrictions	294
PCF Npcf interface settings	296
PCRF Rx interface settings	297
PCF remote SBA nodes	298
RAN configuration settings	300
gNodeB	301
gNodeB Ranges panel	302
gNodeB Range settings	307
gNodeB node settings	308
gNodeB NSSAI settings	310
gNodeB N2 interface settings	311
gNodeB N3 interface settings	313
eNodeB	316
eNodeB Ranges panel	317
eNodeB Range Settings	321
eNodeB Node Settings	321
Passthrough interface settings	323
SBI Fuzzer configuration settings	325
SBI Fuzzer Ranges panel	325
SBI Fuzzer Range panel	325
SBI Fuzzer interface settings	327

SBI Fuzzer Target Node	328
SCP configuration settings	329
SCP Ranges panel	329
SCP Range panel	329
SCP interface settings	331
SCP Remote SBA Nodes	332
SEPP configuration settings	333
SEPP Ranges panel	333
SEPP Range panel	334
SEPP Nsepp interface settings	335
SEPP Remote SBA Nodes	336
SGW configuration settings	338
SGW Ranges panel	339
SGW Range panel	340
SGW S1-U Interface Settings	341
SGW S5-C Interface Settings	342
SGW S5-U Interface Settings	343
SGW S11 Interface Settings	344
SGW DUT S11 Interface Settings	345
SMF/PGW-C configuration settings	346
SMF/PGW-C Ranges panel	347
SMF/PGW-C Range settings	348
SMF node settings	349
SMF N4 interface settings	350
SMF Nsmf interface settings	351
SMF S5-c interface settings	352
SMF remote SBA nodes	353
SMF Uplink Paths	357
SMSF configuration settings	359
SMSF Ranges panel	359
SMSF Range panel	359

SMSF node settings	360
SMSF Nsmsf interface settings	361
SMSF Remote SBA Nodes	362
UDM/HSS configuration settings	364
UDM/HSS Ranges panel	365
UDM/HSS Range panel	366
UDM Range Settings	366
UDM Settings	367
UDM Node Settings	368
UDM Nudm Interface Settings	370
UDM Remote SBA Nodes	371
HSS Range Settings	373
HSS Settings	374
HSS Node Settings	375
HSS S6a Interface Settings	375
UDM and HSS Range Settings	376
UDR configuration settings	377
UDR Ranges panel	377
UDR Range panel	377
UDR Nudr interface settings	378
UDR Remote SBA Nodes	380
UPF/PGW-U configuration settings	381
UPF/PGW-U Ranges panel	382
UPF/PGW-U Range panel	382
UPF N3 interface settings	383
UPF N4 interface settings	384
UPF N6 interface settings	386
UPF N9 interface settings	386
5G-EIR configuration settings	389
5G-EIR Ranges panel	389
5G-EIR Range panel	389

5G-EIR node settings	390
5G-EIR N5g-eir interface settings	390
5G-EIR Remote SBA Nodes	392
NF Discovery service	393
Chapter 8 NG-RAN Simulation tests	395
Chapter 9 SBA tests: configuration settings	396
SBA Tester overview	400
UE configuration settings	401
UE Ranges panel	402
UE Range panel	402
Range Settings	403
UE Identification	404
UE Security	405
UE Settings	407
UE SDF settings	408
Shared Data IDs	408
UE Subscribed AMBR settings	408
Service Area Restrictions	409
Forbidden Areas	410
Notifications	411
Network Slicing	411
UDM Default NSSAI settings	413
UDM SNSSAI Mappings	413
UDR SNSSAI Settings	414
Charging Function	415
Converged Charging	415
Spending Limit Control	416
Objectives	419
Primary Objective	420
About primary objectives	421
Primary Objective Parameters	423

Secondary Objectives	439
UEGetNSSAIAMF2UDM	440
RegistrationAMF2UDM	441
DeregistrationAMF2UDM	442
GetPolicyAMF2PCF	443
UpdatePolicyAMF2PCF	444
GetPolicySMF2PCF	446
UpdatePolicySMF2PCF	447
RegistrationSMF2UDM	449
DeregistrationSMF2UDM	450
IntermediateSpendingLimitPCF2CHF	450
ConvergedChargingUpdateSMF2CHF	451
SBA Tester Global Settings panel	456
Connection Settings	457
Advanced Settings	457
Impairment	459
DNNs panel	460
DNN configuration settings	461
DNN GBR configuration settings	463
Session AMBR configuration settings	463
QoS Flows panel	464
QoS Flow configuration settings	465
QoS Flow Packet Filter configuration settings	467
QoS Flow Maximum Packet Loss configuration settings	468
QoS Flow ARP configuration settings	468
QoS Flow MBR configuration settings	469
QoS Flow GBR configuration settings	469
SBA Tester Simulated Nodes panel	470
AMF configuration settings	470
SMF configuration settings	476
PCF configuration settings	481

SBA Tester Remote SBA Nodes	487
SBA Tester Remote Nodes	489
AUSF configuration settings	491
AUSF Ranges panel	492
AUSF Range panel	492
AUSF node settings	493
AUSF Nausf interface settings	494
AUSF remote SBA nodes	495
CHF configuration settings	497
CHF Ranges panel	497
CHF Range panel	498
CHF node settings	498
CHF Nchf interface settings	499
CHF remote SBA nodes	500
NRF configuration settings	500
NRF Ranges panel	501
NRF Range panel	501
NRF node settings	502
NRF Nnrf interface settings	503
NSSF configuration settings	505
NSSF Ranges panel	506
NSSF Range panel	506
NSSF node settings	507
Nnssf Interface Settings	508
Remote SBA nodes	509
NSSF Restricted NSSAIs	510
NSSF Network Slices	511
NSSF Configured NSSAI	512
PCF configuration settings	513
PCF Ranges panel	513
PCF Range panel	513

PCF node settings	514
PCF service area restrictions	516
PCF Npcf interface settings	517
PCF remote SBA nodes	518
SCP configuration settings	519
SCP Ranges panel	519
SCP Range panel	520
SCP Nscp interface settings	521
SCP Remote SBA Nodes	522
UDM configuration settings	523
UDM Ranges panel	523
UDM Range panel	524
UDM node settings	524
UDM Nudm interface settings	527
UDM remote SBA nodes	529
UDR configuration settings	529
UDR Ranges panel	530
UDR Range panel	530
UDR Nudr interface settings	531
UDR remote SBA nodes	532
Chapter 10 UPF Isolation tests: configuration settings	533
Global Settings panel	536
DNS Settings	537
Advanced Settings	537
Impairment	539
QoS Flows panel	540
QoS Flow configuration settings	540
Reporting Settings	542
UE configuration settings	543
UE Ranges panel	544
UE Range panel	545

UE range settings	546
Objectives	551
Control Plane Objective	551
About primary objectives	552
Primary Control Plane Objective	554
Secondary Control Plane Objectives	556
User Plane Objectives	564
Stateless UDP Traffic Generator	566
Data Traffic	567
Voice Traffic	571
Video OTT Traffic	585
DNS Client Traffic	589
ICMP Client	592
Predefined Applications Traffic	593
Capture Replay	603
DN configuration settings	606
DN Ranges panel	606
DN Range panel	607
DN N6 Interface settings	608
DN routes settings	609
DN User Plane	609
DN Stateless UDP Traffic	610
DN Data Traffic	611
DN Voice Traffic	614
DN Video OTT Traffic	626
DN DNS Server Traffic	628
DN Predefined Applications Traffic	631
DN Capture Replay	631
RAN configuration settings	634
RAN Ranges panel	635
RAN Range settings	635

RAN N3 interface settings	636
Passthrough interface settings	637
SMF configuration settings	638
SMF Ranges panel	639
SMF Range settings	639
SMF N4 interface settings	640
SMF Uplink Paths	642
UPF configuration settings	644
UPF Ranges panel	645
UPF Range panel	645
UPF N3 interface settings	646
UPF N4 interface settings	647
UPF N6 interface settings	649
UPF N9 interface settings	650
UPF N4u interface settings	651
Chapter 11 CoreSim tests: configuration settings	654
Global Settings	658
Global Settings panel	659
Node Start/Stop Rates	659
DNS Settings	660
Advanced Settings	660
DNNs panel	663
DNN configuration settings	663
Session AMBR configuration settings	667
ePCO configuration settings	668
Traffic Control Settings configuration	668
Impairment	669
QoS Flows panel	670
QoS Flow configuration settings	670
QoS Flow Max Packet Loss Rate settings	673
QoS Flow ARP configuration settings	674

QoS Flow MBR configuration settings	674
QoS Flow GBR configuration settings	675
Milenage	675
Customer Parameters	676
CA Certificates	676
UE configuration settings	677
UE Ranges panel	678
UE Range panel	678
Range Settings	680
UE Identification settings	680
UE Security settings	681
UE Settings settings	684
UE Shared Data IDs	689
UE Subscribed AMBR settings	689
Service Area Restriction settings	690
Forbidden Areas	691
DNNs Config	692
Notifications	694
SMS Configuration	695
Equipment Status	696
Converged Charging	697
Spending Limit Control	698
Network Slicing settings	700
UE NSSAI settings	700
UDM Default NSSAI settings	701
UDM SNSSAI Mappings	702
UDR SNSSAI Settings	703
Objectives	704
Control Plane Objective	704
About primary objectives	704
Primary Control Plane Objective	706

Secondary Control Plane Objective	708
User Plane Objectives	715
Stateless UDP Traffic	717
Data Traffic	718
Voice Traffic	722
Video OTT Traffic	736
DNS Client Traffic	740
ICMP Client	743
Ping Traffic	744
Capture Replay	745
Predefined Applications Traffic	747
DN configuration settings	758
DN Ranges panel	758
DN Range panel	759
DN N6 interface settings	760
DN routes settings	761
DN User Plane	762
DN Stateless UDP Traffic	763
DN Data Traffic	764
DN Voice Traffic	766
DN Video OTT Traffic	776
DN DNS Server Traffic	779
DN Predefined Applications Traffic	781
DN Capture Replay	782
IMS configuration settings	785
CSCF Range panel	785
Media Function Range panel	786
RAN configuration settings	787
gNodeB	787
gNodeB Ranges panel	788
gNodeB Range settings	792

gNodeB node settings	793
gNodeB NSSAI settings	795
gNodeB N2 interface settings	796
gNodeB N3 interface settings	800
eNodeB	804
eNodeB Ranges panel	804
eNodeB Range Settings	808
eNodeB Node Settings	809
S1-U Interface Settings	809
S1-MME Interface Settings	811
Passthrough interface settings	812
CoreSim configuration settings	815
Core settings	815
N6/SGi interface settings	816
AMF Ranges configuration settings	817
AMF node settings	819
AMF N2 interface settings	822
UPF Ranges configuration settings	823
UPF N3 interface settings	824
MME Ranges configuration settings	825
MME node settings	826
MME S1 interface settings	827
SGW Ranges configuration settings	828
SGW S1-u interface settings	829
SEG Ranges configuration settings	830
SEG interface settings	834
Chapter 12 Passthrough testing	836
Overview of passthrough testing	837
Passthrough test configuration notes	838
Chapter 13 Troubleshooting	840
Appendix A 5G abbreviations	842

Appendix B Predefined Applications	848
Appendix C Application Actions	862
Index	918

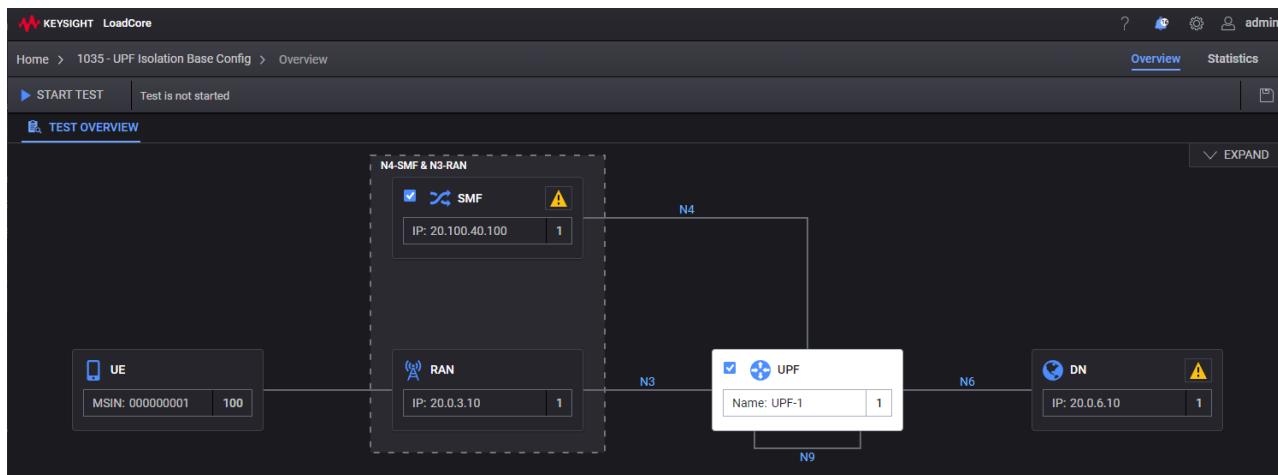
CHAPTER 1

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>).

You can:

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

After activation, the licenses and features will be available in the 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	25
Access LoadCore Web UI	25
LoadCore Web UI	25

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](#).
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
General Settings Menu	<p>The General Settings Menu is located on the top right corner of the Dashboard page. It contains the following menus:</p> <p>The Help Menu can be accessed by selecting the question mark icon on the top right corner of the Dashboard page. Here you can do the following actions:</p> <ul style="list-style-type: none"> • Access LoadCoreHelp where you can find info about the official LoadCore documentation and access the Rest API Browser. • Access Technical Support section, where you can do the following:

Section	Description
	<ul style="list-style-type: none"> ▪ Contact Keysight ▪ Collect diagnostics - for more details refer to Collect Diagnostics. ▪ EULA - select this option to revisit and accept Keysight Software End User License agreement. ▪ Access My software support... ▪ About LoadCore... - this option displays details regarding the LoadCore software version. <p>The Events Menu can be accessed by selecting the bell icon on the top right corner of the Dashboard page. Here you can view notifications and test events.</p> <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"> • License Manager - select this option to open the License Manager section. • Agent Management - select this option to open the Traffic agents management section. • Software Updates - select this option to open the Software Updates section. • Application settings - select this option set or update the license server IP. For more details, refer to Dashboard General Settings. • Administration - select this option to open the Access Control section. <p>The User Profile Menu can be accessed by selecting the user icon on the top right corner of the Dashboard page. Here you can:</p> <ul style="list-style-type: none"> • Access and review your user profile. • Change LoadCore Dashboard theme. For more details, refer to Dashboard General Settings. • Log Out - 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 section allows you to create test sessions based on your test objectives. To create a new test session, select one of the following options:</p> <ul style="list-style-type: none"> • Core topology: <ul style="list-style-type: none"> ▪ Wireless Full Core ▪ Wireless UPF Isolation ▪ Wireless SBA ▪ Wireless CoreSim ▪ Wireless NG-RAN Simulation • O-RAN topology: <ul style="list-style-type: none"> ▪ Wireless CoreSim

Section	Description
	<ul style="list-style-type: none"> ▪ Wireless CuSIM ▪ Wireless DuSIM <p>Selecting one of the options above will create a new session with that type of topology loaded.</p> <p>IMPORTANT For Wireless CuSIM and Wireless DuSIM configuration, refer to the related documentation available on Keysight's support page. For the rest of the topologies listed above, the steps required for configuration are described in the Configure and run a test section.</p>
Browse Configs	<p>This section allows you to manage previously configured test sessions. 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	<p>This section allows you to access previous sessions results, view detailed reports and export results.</p>
Online resources	<p>This section contains links to the official LoadCore documentation.</p>

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 the Web UI](#).

You can perform the following actions from LoadCore:

Configure and run a test	29
Create test scenarios	34
Work with saved test configurations	34
Licensed Test Configs	40
Upgrade the MiddleWare VM	57
Configure Dashboard general settings	58
Configure LoadCore with LDAP/AD	59
Reset Password for Regular Users	63
Debug	65
View Notifications and Test Events	65
View Statistics	66
Manage Test Results	67
Collect Diagnostics	67

Configure and run a test

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

- [Configure a Wireless Full Core test](#)
- [Configure a Wireless UPF Isolation test](#)
- [Configure a Wireless SBA test](#)
- [Configure Wireless NG-RAN Simulation test](#)
- [Configure Wireless CoreSim test](#)

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 panel](#).
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:

- [Access and Mobility Management Function \(AMF\)](#)
- [Authentication Server Function \(AUSF\)](#)
- [Charging Function \(CHF\)](#)
- [Data Networks \(DN\)](#)
- [DNS Server](#)

- [Equipment Identity Register \(5G-EIR\)](#)
- [IP Multimedia Subsystem \(IMS\)](#)
- [Mobility Management Entity \(MME\)](#)
- [Network Exposure Function \(NEF\)](#)
- [Network Repository Function \(NRF\)](#)
- [Network Slice Selection Function \(NSSF\)](#)
- [Policy Control Function \(PCF/PCRF\)](#)
- [Radio Access Network \(RAN\)](#)
- [SBI Fuzzing](#)
- [Service Communication Proxy \(SCP\)](#)
- [Security Edge Protection Proxy \(SEPP\)](#)
- [Serving Gateway \(SGW\)](#)
- [Session Management Function \(SMF/PGW-C\)](#)
- [Short Message Service Function \(SMSF\)](#)
- [Unified Data Management \(UDM/HSS\)](#)
- [Unified Data Repository \(UDR\)](#)
- [User Plane Function \(UPF/PGW-U\)](#)

5. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic Agents](#).
6. Configure the test settings for the simulated UEs. While there are a large number of UE configuration settings, you can often use the default values with little or no modification. For UE configuration, refer to [User Equipment \(UE\)](#).
7. On the [User Equipment \(UE\)](#), configure the test objectives. The test *Objectives* determine the behavior of the simulated UEs. The User Plane Objectives determine the volume and rate of data traffic, and The Control Plane Objectives determine the volume and rate of control plane procedures.
8. Start the test. When you click or tap the **Start Test** button, 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](#).
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:

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

5. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic Agents](#).
6. Configure the test settings for the simulated UEs. While there are a large number of UE configuration settings, you can often use the default values with little or no modification.
For UE configuration, refer to [User Equipment \(UE\)](#).
7. On the [User Equipment \(UE\)](#), configure the test objectives.
The test *Objectives* determine the behavior of the simulated UEs. The User Plane Objectives determine the volume and rate of data traffic, and The Control Plane Objectives determine the volume and rate of control plane procedures.
8. Start the test. When you click or tap the **Start Test** button, 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 [Global Settings panel](#).

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

5. Configure the test settings for the SBA tester node and simulated nodes. For more details, refer to SBA tests: configuration settings.

6. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic Agents](#).

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.

Configure Wireless NG-RAN Simulation test

The NG-RAN simulation test is a Full Core test topology simulation that has all the nodes disabled, except NG-RAN, and the AMF and UPF nodes are configured as DUTs. You can enable other nodes based on your test objectives.

To configure this test, on the LoadCore Dashboard page, under the Create New Test section, select **Wireless NG-RAN Simulation**. The Test Scenario page appears.

The Test Scenario configuration is similar with the Full Core test one, so for more details regarding the test set-up work-flow, refer to [Configure a Wireless Full Core test](#).

Configure Wireless CoreSim test

To configure this test, do the following:

1. On the LoadCore Dashboard page, under the Create New Test section, select **Wireless CoreSim**.
The Test Scenario page appears.
2. On the Test Overview panel configure Global Settings. These settings become immediately available for selection in several of the node configuration windows. You define them once and reuse them multiple times.
For more details about Global Settings configuration, refer to [Global Settings panel](#).
3. Select the services and nodes that the 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:

- [CoreSim](#)
- [Data Networks \(DN\)](#)
- [IP Multimedia Subsystem \(IMS\)](#)
- [Radio Access Network \(RAN\)](#)

5. Select the number of traffic agents for each LoadCore node. For more details, refer to [Traffic Agents](#).
6. Configure the test settings for the simulated UEs. While there are a large number of UE configuration settings, you can often use the default values with little or no modification.
For UE configuration, refer to [User Equipment \(UE\)](#).
7. On the [User Equipment \(UE\)](#), configure the test objectives.
The test *Objectives* determine the behavior of the simulated UEs. The User Plane Objectives determine the volume and rate of data traffic, and The Control Plane Objectives determine the volume and rate of control plane procedures.

8. Start the test. When you click or tap the **Start Test** button, 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

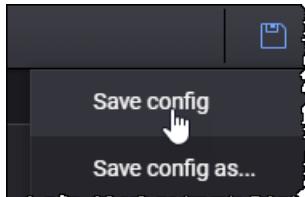
If there are multiple test sessions, you can quickly switch between them by selecting the small green triangle next to the name of the current test session. A drop-down list will displays all your current test sessions and allows you to change to a specific test session by selecting it.

Create test scenarios

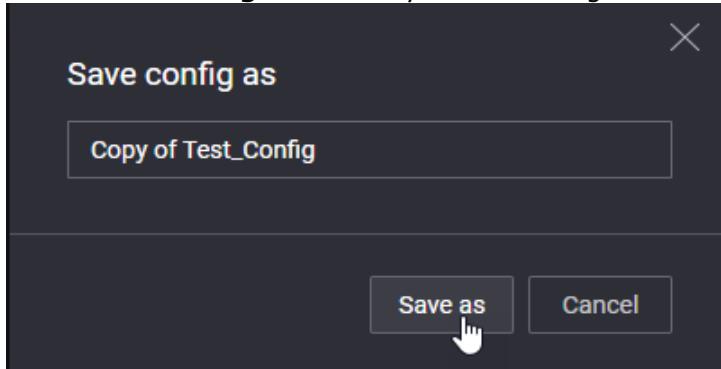
Once a test is configured (for details, refer to [Configure a test](#)), you can record its configuration as a scenario, edit and save it for future use.

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 config as** 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 as**.

Work with saved test configurations

This topic describes how to work with saved test configurations.

- [The Browse Configs dashboard](#)
- [Import a saved test configuration from disk](#)
- [Create a test session based on licensed test configuration](#)

- [Delete a saved test configuration](#)
- [Export a saved test configuration](#)

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.

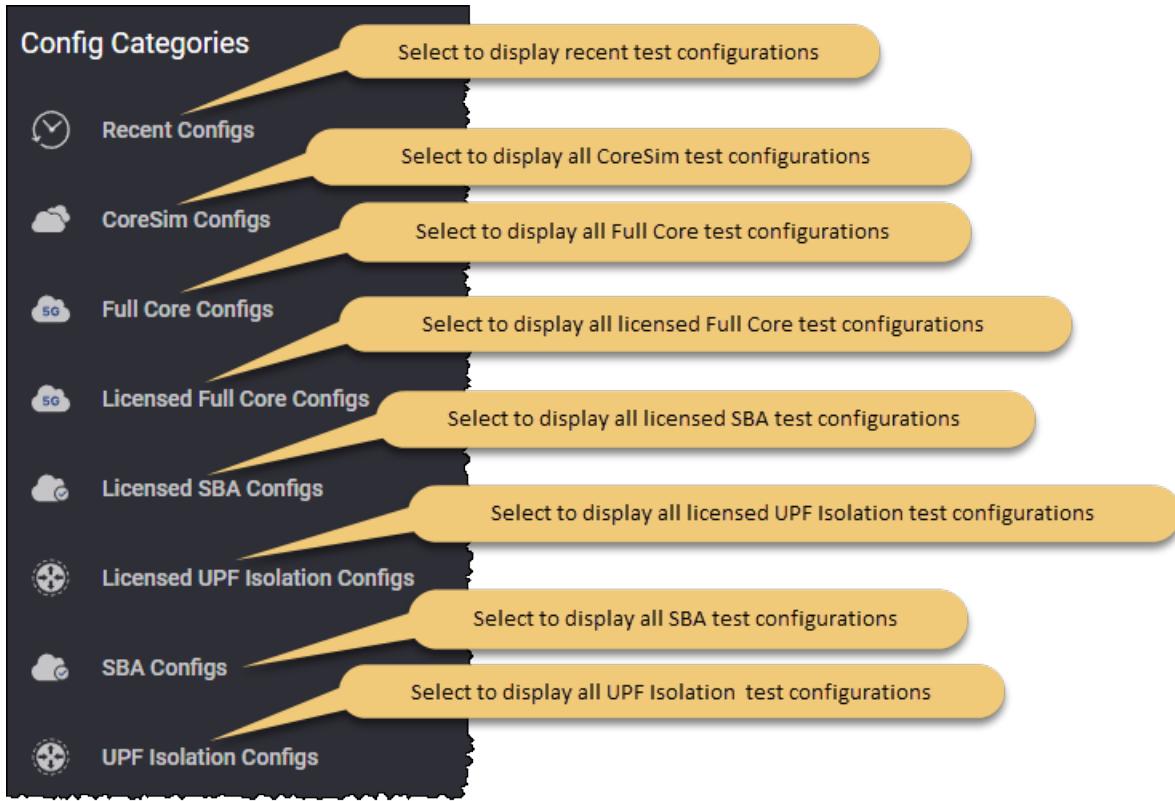
NOTE If the selected configuration is already opened in an existing session, a message is displayed allowing you to open that session or to create a new session based on the selected test configuration.

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

- [Test configuration categories](#)
- [Test configuration areas](#)

Test configuration categories

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



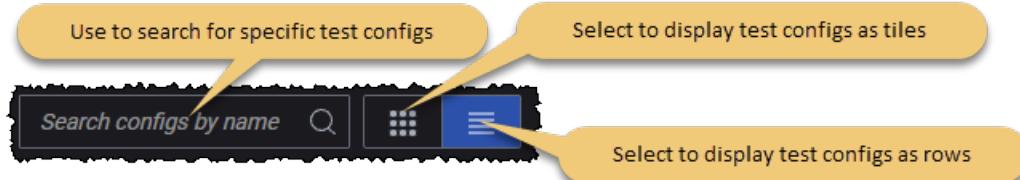
Also, you can add test configurations on the dashboard by importing them or export the existing ones.



Test configuration areas

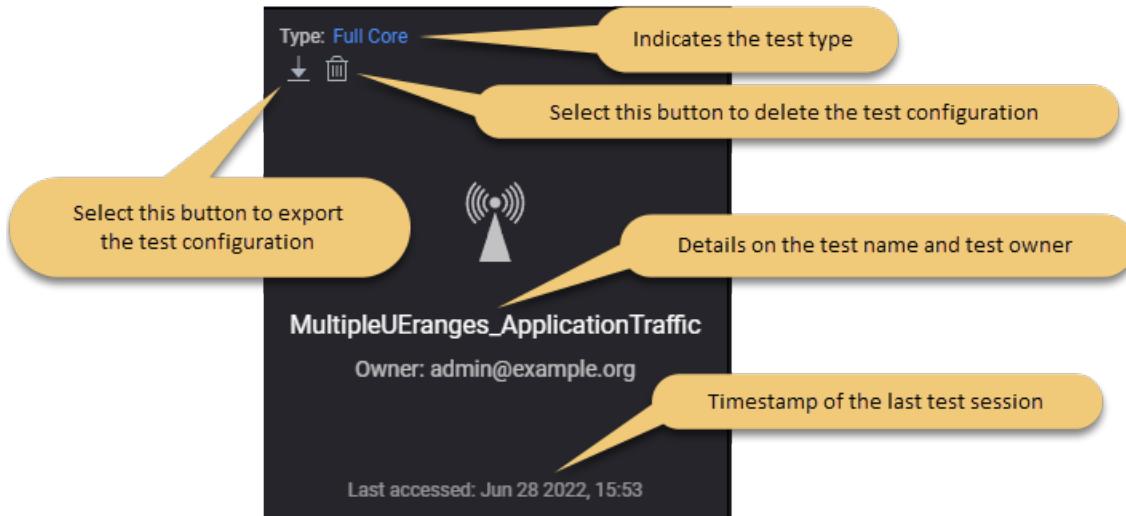
On this area, LoadCore displays your test configurations suite, offering you details on the specific test configuration and allowing you to delete it or to export it.

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	Timestamp of the last test session	Application	Config Type	Owner	Create Session
<input type="checkbox"/> fullcore_ipv6_multi_agents	Jun 28, 2022, 3:53:21 PM	Full Core	Full Core	admin@example.org	
<input type="checkbox"/> fullcore_ipv6_multi_agents (copy from Mar 15 10:44:36)	Jun 28, 2022, 3:53:21 PM	Full Core	Full Core	admin@example.org	
<input type="checkbox"/> fullCore_SRIOV_dpdk_CPV4_UPv4_http_GtpuSourcePortCount_4	Jun 28, 2022, 3:53:19 PM	Full Core	Full Core	admin@example.org	
<input type="checkbox"/> fullCore_Tiger_allTrafficFlows (copy from Jun 28 12:52:13)	Jun 28, 2022, 3:52:15 PM	Full Core	Full Core	admin@example.org	
<input checked="" type="checkbox"/> Full Core Base Config	Jun 28, 2022, 3:51:33 PM	Full Core	Full Core	system	
<input type="checkbox"/> fullcore_Tiger_putHttpTraffic	Jun 28, 2022, 3:51:04 PM	Full Core	Full Core	admin@example.org	

Annotations for the table:

- A yellow callout points to the "Config Name" column header with the text "Use to select a test configuration".
- A yellow callout points to the "Timestamp of the last test session" column header with the text "Timestamp of the last test session".
- A yellow callout points to the "Owner" column header with the text "Indicates the test owner".
- A yellow callout points to the "Create Session" column header with the text "Select to create a test session based on this configuration".
- A yellow callout points to the "Delete" button at the bottom left with the text "Select this button to delete the test configuration".
- A yellow callout points to the "Export" button at the bottom left with the text "Select this button to export the test configuration".
- A yellow callout points to the "fullcore_ipv6_multi_agents" row with the text "Details on the test name".
- A yellow callout points to the "fullCore_SRIOV_dpdk_CPV4_UPv4_http_GtpuSourcePortCount_4" row with the text "Indicates a base configuration".

A new wireless test has five base configurations:

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

For example ...

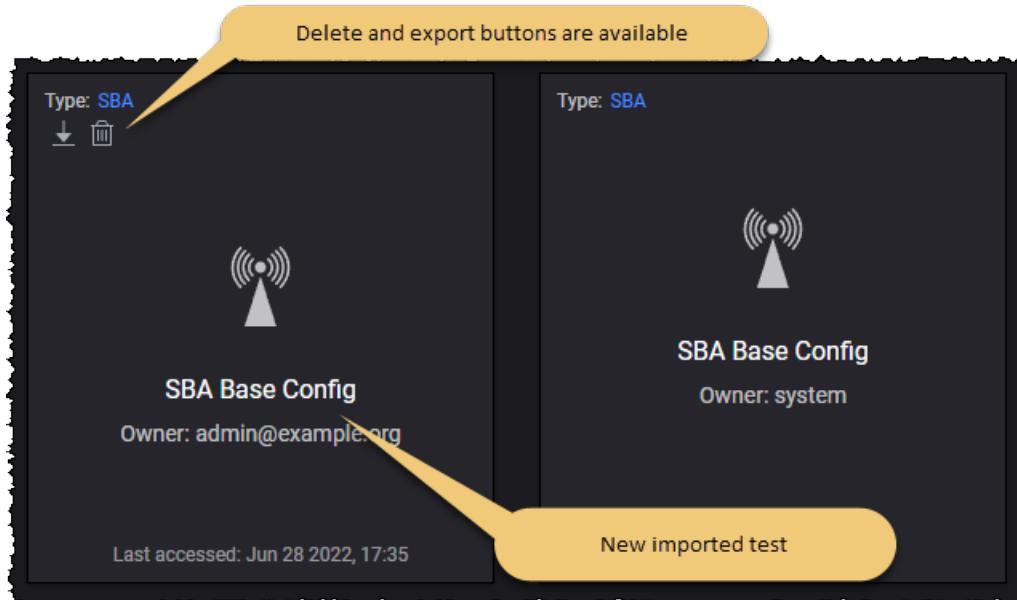
Type: Full Core Full Core Base Config Owner: system	Type: SBA SBA Base Config Owner: system	Type: Full Core NG-RAN Simulation Base Config Owner: system	Type: UPF Isolation UPF Isolation Base Config Owner: system	Type: CoreSim CoreSim Base Config Owner: system
---	---	---	---	---

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 ...

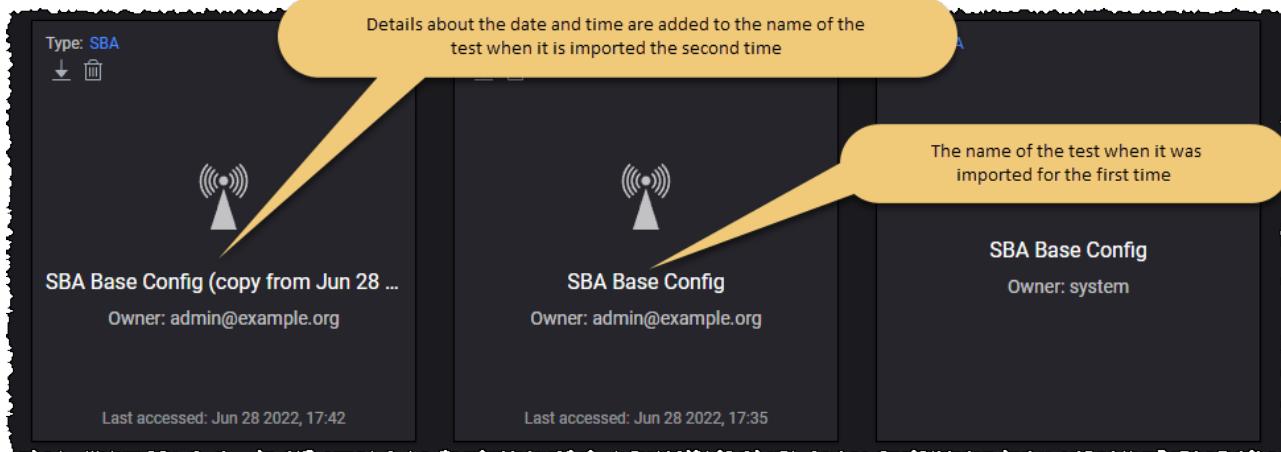


The new imported test is a user test that has the delete and export buttons on the top-right corner of the test tile.

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, the other tests will 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.

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

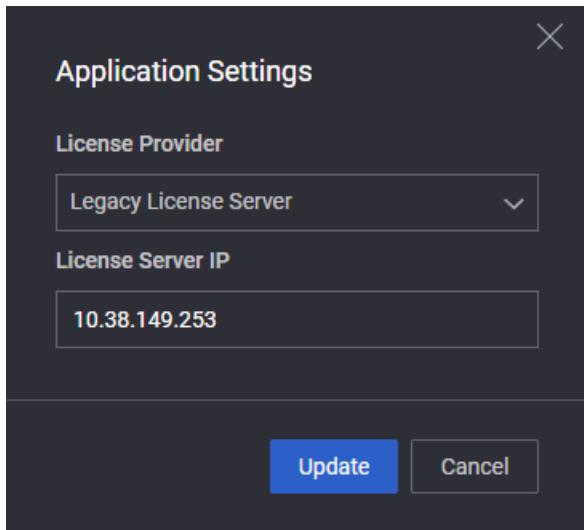
This section displays info related to the current installed software version of LoadCore.

To update to a newer version, do the following:

1. Select the wheel icon > **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 (using the old LicenseManager).

- **External License Server** - select this option to set an external license server (using the new LicenseManager 1.7 available with the LoadCore 3.2 release).
- **Embedded License Server** - the license server that is included in LoadCore MW. If you want to activate licenses, go to wheel icon > [Application Settings](#).

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 user profile icon on the top right corner of the Dashboard page. The user settings menu appears.
2. From the user settings menu, select **Preferences > Switch Theme**.

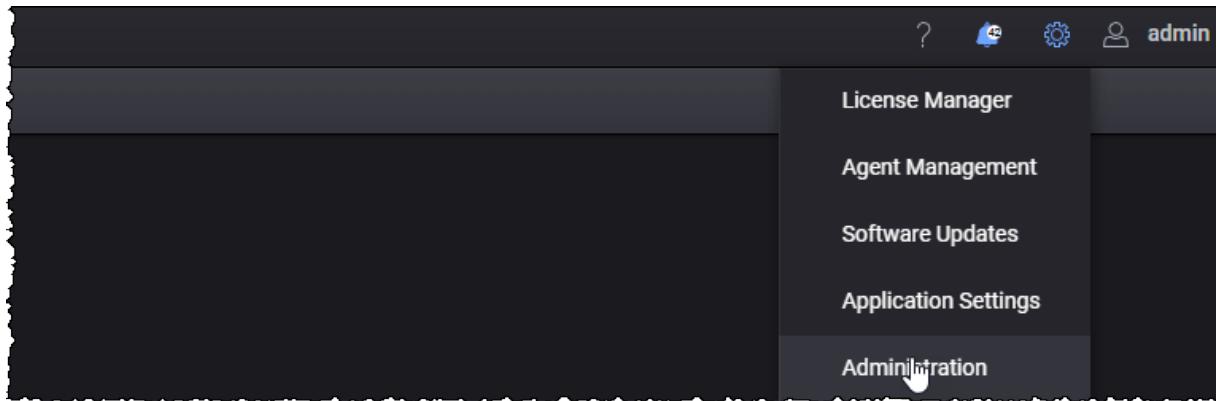
Log out

To log out of the LoadCore browser-based Web UI, select the user profile menu from the upper-right corner of the Dashboard page and select **Log Out**. 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**.



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.

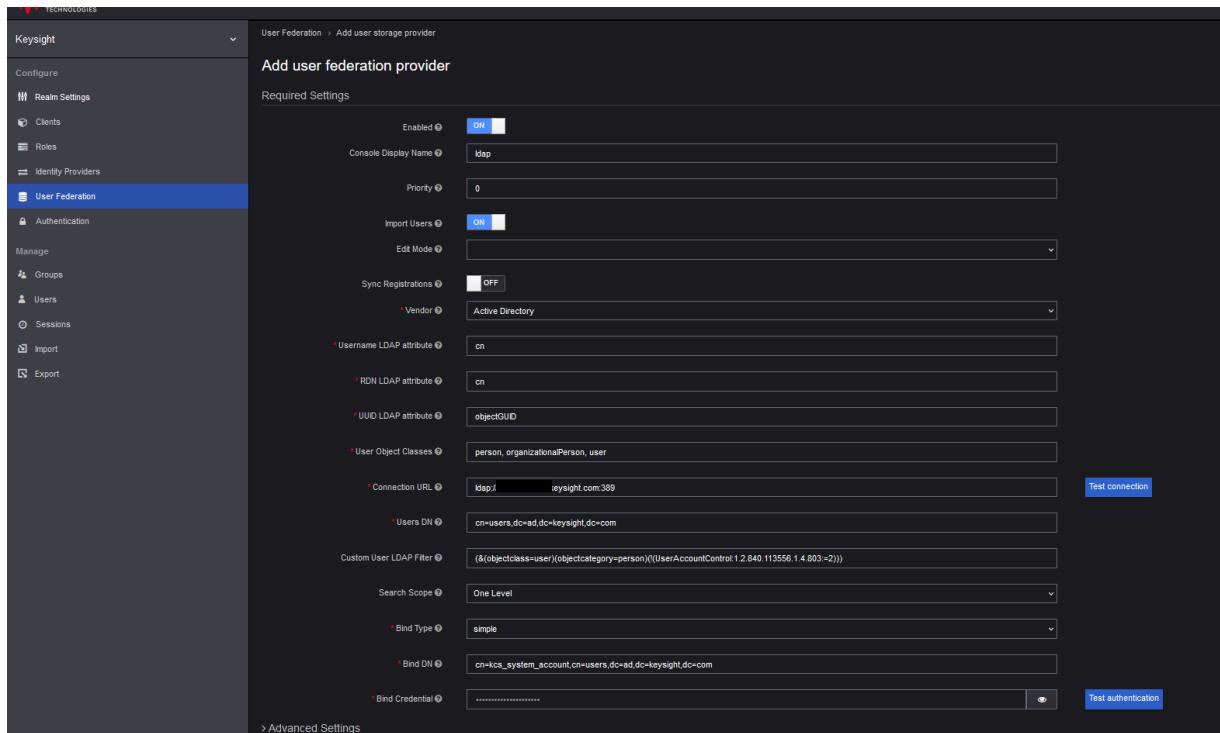
Then, to make it as a default group:

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	!

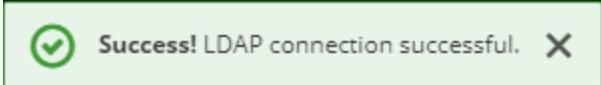
For Example:

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

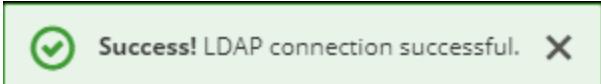
It reduced Users number from 26185 to 21262 in Keysight Active Directory on 10/12/2020.

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.



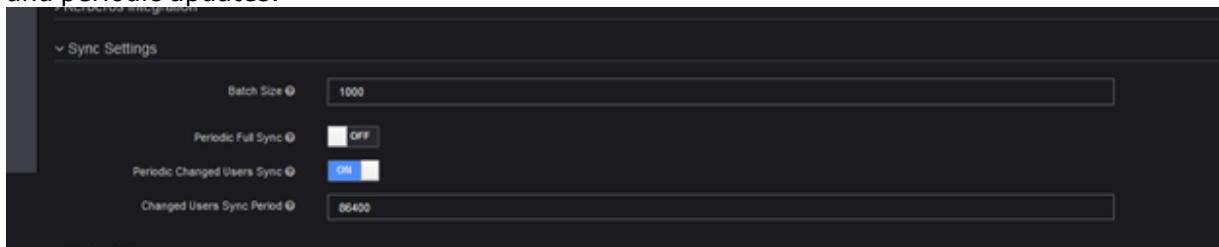
- **Test Authentication** - This button allows you to test if connection is correctly authenticated. After selecting the **Test Authentication** button success is indicated by a success message on the top of the page.



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.



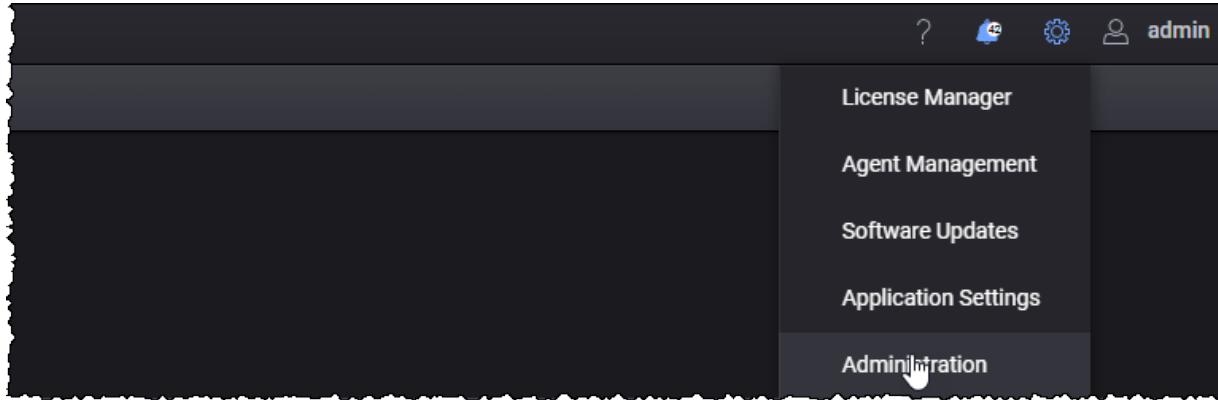
IMPORTANT It takes a long time to do a full synchronization. Wait until the success or failed message is displayed.

Reset Password for Regular Users

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

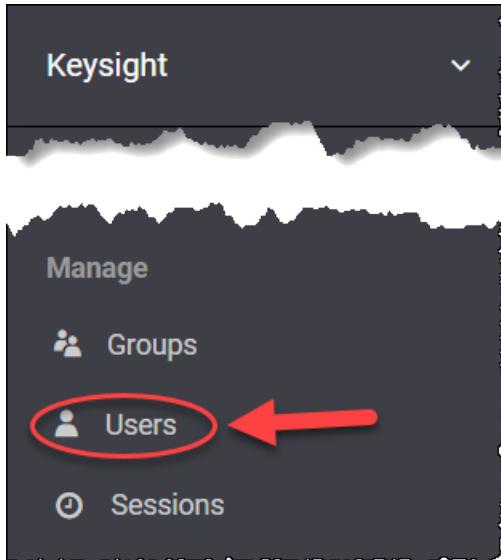
IMPORTANT The password can be changed only by an **ADMIN** user.

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



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

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



The Users section is displayed.

3. 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.

The screenshot shows the AWS IAM 'Users' page. There are two users listed: 'admin' and 'tester'. The 'Edit' button for the 'tester' user is highlighted with a red circle.

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.

4. Select **Credentials**.

The screenshot shows the 'User Details' page for the 'tester' user. The 'Credentials' tab is selected and highlighted with a red circle. The user information shown includes ID, Created At, and Username.

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

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

The screenshot shows the 'User Details' page for the 'tester' user. The 'Credentials' tab is selected. In the 'Set Password' section, the 'Temporary' switch is turned 'ON'. The 'Set Password' button is highlighted with a red circle.

Debug

LoadCore offers support for debugging capabilities so that you can:

- [View Events](#)
- [View Statistics](#)
- [Collect Diagnostics](#)

View Notifications and Test Events

The navigationbar displays a notifications icon  and a counter showing the total number of triggered notifications since the counter was last reset for the current LoadCoreinstance. The icon and the counter are visible from all the pages of the LoadCore web UI. The notification icon 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 a notification is triggered, a color-coded banner is also displayed on the lower right corner of the screen: green for informational messages, orange for messages informing you of actions you are not allowed to perform, and red for error messages.

NOTE While on the Dashboard page, the notifications icon displays notifications strictly at cluster/system level.

NOTE While inside a test session, the notifications icon displays notifications for the currents test and notifications at the cluster and system level.

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

Here you can view details on the registered events regarding the logging date, their severity type and description. You can 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 dialog titled "Events". At the top, there are four filter checkboxes: "All" (checked), "Info" (checked), "Warning" (checked), and "Error" (unchecked). Below the filters is a table with three columns: "Date ^", "Type", and "Message". The table contains six rows, each representing a successful import of 1 configuration at different times on June 28, 2022. At the bottom right of the dialog are two buttons: "Go to events page" and "Close".

Date ^	Type	Message
Jun 28, 2022, 5:22:25 PM	<i>INFO</i>	Successfully imported 1 configurations
Jun 28, 2022, 5:22:28 PM	<i>INFO</i>	Successfully imported 1 configurations
Jun 28, 2022, 5:23:23 PM	<i>INFO</i>	Successfully imported 1 configurations
Jun 28, 2022, 5:23:24 PM	<i>INFO</i>	Successfully imported 1 configurations
Jun 28, 2022, 5:23:27 PM	<i>INFO</i>	Successfully imported 1 configurations
Jun 28, 2022, 5:24:20 PM	<i>INFO</i>	Successfully imported 1 configurations

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

The screenshot shows the "Events" page within the LoadCore web interface. At the top, there is a header with the Keysight logo, "LoadCore", and user navigation links. Below the header, a breadcrumb trail shows "Home > Events". On the left, there is a "Filter events by" section with a "Message" input field containing "Type keywords" and a search icon. To the right of the input field are four filter checkboxes: "All" (checked), "Info" (checked), "Warning" (checked), and "Error" (unchecked). Below the filter section is a table with three columns: "Date ^", "Type", and "Message". The table lists seven rows of imported configurations from June 24, 2022, all of which are of type "INFO" and message "Successfully imported 1 configurations".

Date ^	Type	Message
Jun 24, 2022, 11:23:40 AM	<i>INFO</i>	Successfully imported 1 configurations
Jun 24, 2022, 11:23:41 AM	<i>INFO</i>	Successfully imported 1 configurations
Jun 24, 2022, 11:23:47 AM	<i>INFO</i>	Successfully imported 1 configurations
Jun 24, 2022, 11:23:47 AM	<i>INFO</i>	Successfully imported 1 configurations
Jun 24, 2022, 11:25:20 AM	<i>INFO</i>	Successfully imported 1 configurations
Jun 24, 2022, 11:25:21 AM	<i>INFO</i>	Successfully imported 1 configurations

Here you can search for events based on the available filtering criteria.

View Statistics

After you access the LoadCore web UI, create a test session or enter an existing test session, configure and start the test, you can view the real-time statistics on the **STATISTICS** page.

Manage 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.
 - Delete the test results, by selecting the **Delete** button.
- NOTE** To download the captures you need to enable traffic capture on the test agents.
- 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).

Collect Diagnostics

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

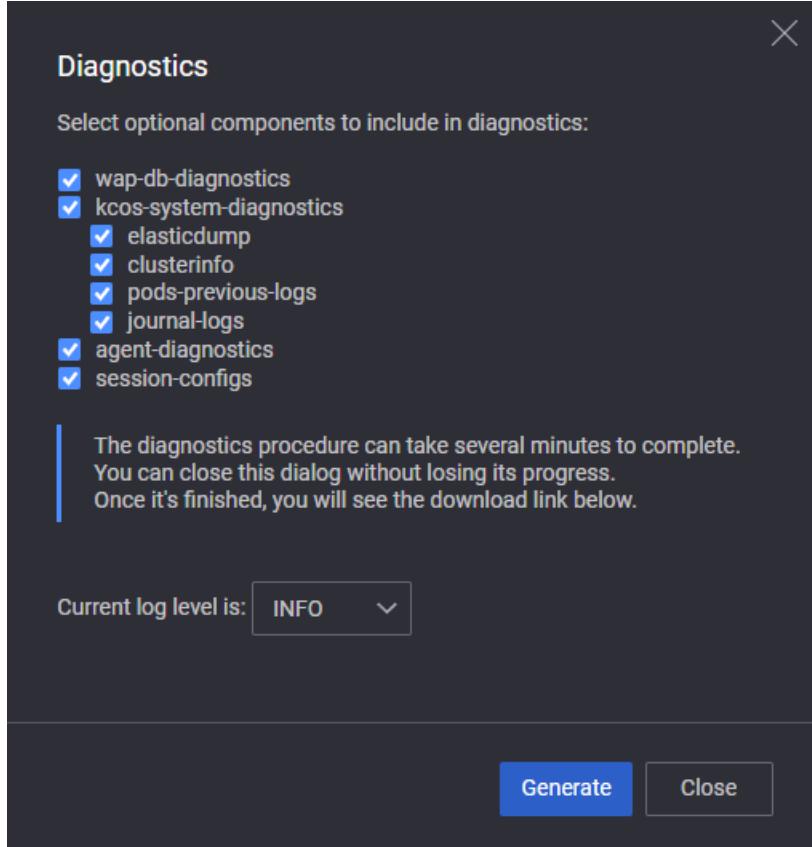
To collect diagnostics, do the following:

1. Select the Help menu (question mark icon) > **Collect Diagnostics**. The Diagnostics window appears.
2. If needed, select the optional components to include in the diagnostics report.
3. Select 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 ...



CHAPTER 5

License Manager

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

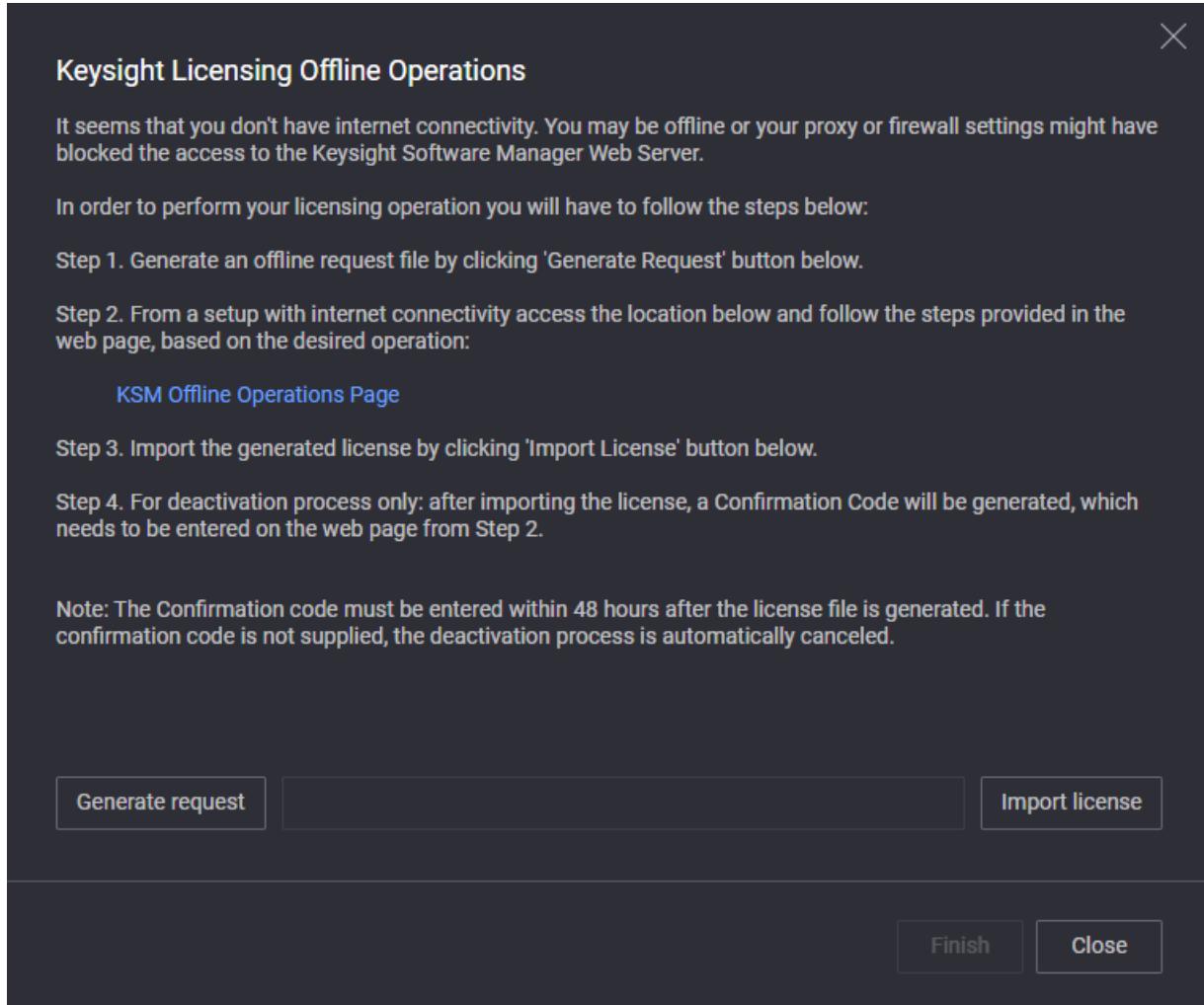
The screenshot shows the LoadCore License Manager interface. At the top, there's a navigation bar with the KEYSIGHT LoadCore logo, a search icon, a bell icon, a gear icon, and a user account icon labeled "admin". Below the navigation bar, the page title is "Home > License Manager". A table header row contains columns for "Part ID", "Product", "Description", "License Expiration", "Maintenance Expiration", "Activation Code", "Quantity", and "Manage Reservation". A message below the table states "There are no licenses available." At the bottom of the screen, there are four buttons: "Activate licenses", "Sync licenses", "Offline operations", and "License statistics", followed by a "Deactivate licenses" button.

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 header "Activate Licenses" with a close button. Below the header is a section for "Enter License Data:" containing an "Example:" field with sample activation codes: "889D-0CB0-BC3D-3179, 10", "F5A5-CA75-1AED-C0AC, 5", and "23a9798736-347903a1-b1ad4788-cfa78bb7-b17c98d7-90232753". There is a "Load data" button next to this section. Below this is a section for "Select and edit activation codes:" with a table header row containing columns for "Product", "Description", "Activation Code", "Entitlement Code", "Total", "Available", and "To Activate". The table body is currently empty. At the bottom right of the dialog box are "Activate" and "Close" buttons.

- **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.



- **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 6

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 screenshot shows the 'Agents Assignment' window under 'Network Management'. On the left, a sidebar lists various network components: NRF, AUSF, PCF/PCRF, UDR, NSSF, SMSF, CHF, AMF, UDM/HSS, SMF/PGW-C, RAN, UPF/PGW-U, and DN. The main area is titled 'AUSF Agents Assignment (8)' and shows '1 agent selected'. A filter bar allows filtering by agents. The table has columns: 'Owner' (with a checkmark for 10.38.154.203), 'Select Agent' (checkboxes for all agents), 'Tags' (including 'hostname: 5... (8)', 'lxStack: OFF (5)', 'build: pipelin... (8)'), 'Hostname' (5GCTE-7008b9fa51 for all), and 'Connections' (Nauf, with dropdown menus for each agent). At the bottom right are 'Update' and 'Cancel' buttons.

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>
Hostname	Displays the hostname.
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	lxStack: 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	lxStack: 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	lxStack: 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	This column displays the tags associated to each agent. There are two types of tags: <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. Each tag indicates the number of agents to which it was associated.
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>The SRIOV setting can be used freely in most types of setups and is not exclusive to SRIOV/VF interfaces. With it enabled, the test interface uses the MAC address of the NIC, instead of the address configured in the LoadCore UI on the protocol interface (N2, N3, S1 ...).</p> <p>This is useful both in on premise and in cloud setups, since it eliminates the need to configure extra trust/security relations between the LoadCore agents/DUT network.</p> <p>The SRIOV setting is enabled by default. It is disabled when <i>Network Stack</i> is set to Linux Stack and is not available for SBA topology since it does not allow IxStack.</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.

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 > **Agent Management**.

For example ...

Agent Management (8)											
				CPU info							
Agent IP	Owner	Status	Tags	Test NICs	Hostname	Memory	Model	Frequency	Cores	Last Run Data	Last Run Timestamp
<input type="checkbox"/> 10.38.149.206		Stopped	IxStack: OFF (6) build: pipeline... (8)	ens160 ens192	5GCTE-18631b0770	7.79 GB	Intel®	3.5 GHz	4	Full Core(ng-ran,amf,upf,ssf,ausf,udm,pcf,udr,smf)	Jun 30, 2022, 10:28:30 AM
<input type="checkbox"/> 10.38.149.207		Stopped	IxStack: OFF (6) build: pipeline... (8)	ens192 ens160	5GCTE-18631b0770	3.85 GB	Intel®	3.5 GHz	4	Full Core(ng-ran)	Jun 30, 2022, 2:49:03 PM
<input type="checkbox"/> 10.38.149.208		Stopped	IxStack: OFF (6) build: pipeline... (8)	ens192 ens160	5GCTE-18631b0770	3.85 GB	Intel®	3.5 GHz	4	Full Core(amf,upf,ausf,udm,pcf,udr,smf)	Jun 30, 2022, 2:49:02 PM
<input type="checkbox"/> 10.38.149.211		Stopped	IxStack: OFF (6) build: pipeline... (8)	ens192 ens160	5GCTE-18631b0770	7.79 GB	Intel®	3.5 GHz	4	UPF Isolation(upf)	Jun 29, 2022, 4:25:07 AM
<input type="checkbox"/> 10.38.154.198		Stopped	IxStack: OFF (6) build: pipeline... (8)	ens4 ens9	5GCTE-18631b0770	31.41 GB	Intel	2.3 GHz	16	SBA(chf)	Jun 30, 2022, 2:36:13 PM
<input type="checkbox"/> 10.38.154.201		Stopped	IxStack: OFF (6) build: pipeline... (8)	ens9 ens4	5GCTE-18631b0770	31.41 GB	Intel	2.3 GHz	16	SBA(generic-sba-tester)	Jun 30, 2022, 2:36:14 PM
<input type="checkbox"/> 10.38.158.254		Running	IxStack: ON (2) DPDK (2) build: pipeline... (8)	enp6s0 enp3s0	5GCTE-18631b0770	7.79 GB	Intel	3.6 GHz	4	UPF Isolation(upf)	Jun 30, 2022, 2:37:30 PM
<input type="checkbox"/> 10.38.159.1		Running	IxStack: ON (2) DPDK (2) build: pipeline... (8)	enp3s0 enp6s0	5GCTE-18631b0770	7.79 GB	Intel	3.6 GHz	4	UPF Isolation(n4-smf)	Jun 30, 2022, 2:37:30 PM

Clear Ownership Hard Reboot Soft 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: <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. Each tag indicates the number of agents to which it was associated.
Test NICs	Displays the NICs for each agent and on hover it displays the MAC address 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.

Column	Description
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.

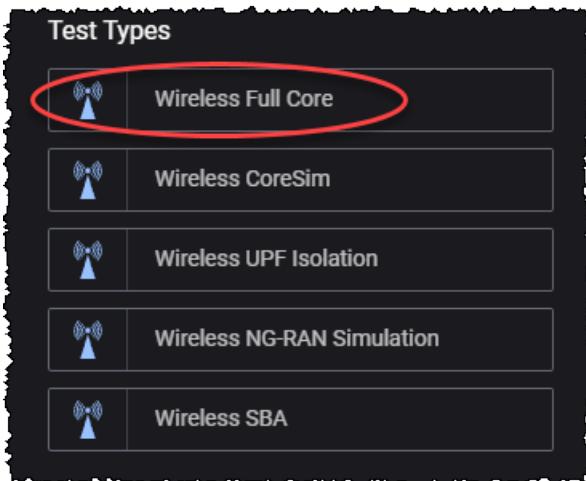
When you select one or more agents, the following actions became available:

- **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 7

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	85
Global Settings panel	87
Node Start/Stop Rates	87
DNS Settings	88
Advanced Settings	88
DNNs panel	93
DNN configuration settings	94
Session AMBR configuration settings	97
ePCO configuration settings	98
Traffic Control Settings configuration	98

Impairment	99
QoS Flows panel	100
QoS Flow configuration settings	101
QoS Flow Max Packet Loss Rate settings	103
QoS Flow ARP configuration settings	104
QoS Flow MBR configuration settings	104
QoS Flow GBR configuration settings	105
Milenage	105
Customer Parameters	106
CA Certificates	106
UE configuration settings	107
UE Ranges panel	108
UE Range panel	109
Range Settings	111
UE Identification settings	112
UE Security settings	112
UE Settings settings	116
UE Shared Data IDs	120
UE Subscribed AMBR settings	120
Service Area Restriction settings	120
Forbidden Areas	122
DNNs Config	123
Notifications	126
SMS Configuration	126
Equipment Status	127
Converged Charging	128
Spending Limit Control	129
Internal Group IDs	131
Network Slicing settings	133
UE NSSAI settings	134
UDM Default NSSAI settings	135
UDM SNSSAI Mappings	135

UDR SNSSAI Settings	136
Objectives	137
Control Plane Objective	138
About primary objectives	139
Primary Control Plane Objective	141
Secondary Control Plane Objective	143
User Plane Objectives	153
Stateless UDP Traffic	154
Data Traffic	155
Voice Traffic	159
Video OTT Traffic	173
DNS Client Traffic	176
ICMP Client	179
Ping Traffic	180
Capture Replay	181
Predefined Applications Traffic	183
AMF configuration settings	194
AMF Ranges panel	195
AMF Range settings	196
AMF node settings	197
AMF N2 interface settings	200
AMF Namf interface settings	201
AMF N26 Interface Settings	202
AMF remote SBA nodes	203
AUSF configuration settings	210
AUSF Ranges panel	211
AUSF Range panel	211
AUSF node settings	212
AUSF Nausf interface settings	213
AUSF Remote SBA Nodes	214
CHF configuration settings	217
CHF Ranges panel	217

CHF Range settings	218
CHF node settings	219
CHF Nchf interface settings	219
CHF remote SBA nodes	220
DN configuration settings	222
DN Ranges panel	223
DN Range panel	223
DN N6 interface settings	224
DN routes settings	225
DN User Plane	226
DN Stateless UDP Traffic	227
DN Data Traffic	228
DN Voice Traffic	231
DN Video OTT Traffic	241
DN DNS Server Traffic	244
DN Predefined Applications Traffic	246
DN Capture Replay	247
DNS Server configuration settings	250
DNS Server Ranges panel	250
DNS Server Range panel	250
DNS Server Ndnnserver interface settings	251
DNS Server Traffic Flow settings	252
IMS configuration settings	255
CSCF Range panel	255
CSCF N6 interface settings	256
CSCF Rx interface settings	257
CSCF UE routes settings	258
Media Function Range panel	259
MME configuration settings	261
MME Ranges panel	262
MME Range panel	263
MME node settings	264

MME S11 Interface Settings	265
MME N26 Interface Settings	266
MME S1 Interface Settings	267
MME S6a Interface Settings	269
MME Diameter settings	270
NEF configuration settings	271
NEF Ranges panel	271
NEF Range panel	271
NEF Nnef interface settings	272
NEF Remote SBA Nodes	273
NRF configuration settings	276
NRF Ranges panel	277
NRF Range panel	277
NRF node settings	278
NRF Nnrf interface settings	279
NRF Remote SBA Nodes	280
NSSF configuration settings	282
NSSF Ranges panel	283
NSSF Range panel	283
NSSF node settings	284
Nnssf Interface Settings	285
Remote SBA nodes	286
NSSF Restricted NSSAIs	287
NSSF Network Slices	288
NSSF Configured NSSAI	289
PCF/PCRF configuration settings	290
PCF/PCRF Ranges panel	291
PCF Range panel	292
PCF node settings	293
PCRF node settings	294
PCF service area restrictions	294
PCF Npcf interface settings	296

PCRF Rx interface settings	297
PCF remote SBA nodes	298
RAN configuration settings	300
gNodeB	301
gNodeB Ranges panel	302
gNodeB Range settings	307
gNodeB node settings	308
gNodeB NSSAI settings	310
gNodeB N2 interface settings	311
gNodeB N3 interface settings	313
eNodeB	316
eNodeB Ranges panel	317
eNodeB Range Settings	321
eNodeB Node Settings	321
Passthrough interface settings	323
SBI Fuzzer configuration settings	325
SBI Fuzzer Ranges panel	325
SBI Fuzzer Range panel	325
SBI Fuzzer interface settings	327
SBI Fuzzer Target Node	328
SCP configuration settings	329
SCP Ranges panel	329
SCP Range panel	329
SCP interface settings	331
SCP Remote SBA Nodes	332
SEPP configuration settings	333
SEPP Ranges panel	333
SEPP Range panel	334
SEPP Nsepp interface settings	335
SEPP Remote SBA Nodes	336
SGW configuration settings	338
SGW Ranges panel	339

SGW Range panel	340
SGW S1-U Interface Settings	341
SGW S5-C Interface Settings	342
SGW S5-U Interface Settings	343
SGW S11 Interface Settings	344
SGW DUT S11 Interface Settings	345
SMF/PGW-C configuration settings	346
SMF/PGW-C Ranges panel	347
SMF/PGW-C Range settings	348
SMF node settings	349
SMF N4 interface settings	350
SMF Nsmf interface settings	351
SMF S5-c interface settings	352
SMF remote SBA nodes	353
SMF Uplink Paths	357
SMSF configuration settings	359
SMSF Ranges panel	359
SMSF Range panel	359
SMSF node settings	360
SMSF Nsmsf interface settings	361
SMSF Remote SBA Nodes	362
UDM/HSS configuration settings	364
UDM/HSS Ranges panel	365
UDM/HSS Range panel	366
UDM Range Settings	366
UDM Settings	367
UDM Node Settings	368
UDM Nudm Interface Settings	370
UDM Remote SBA Nodes	371
HSS Range Settings	373
HSS Settings	374
HSS Node Settings	375

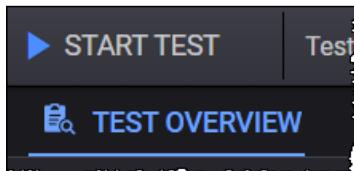
HSS S6a Interface Settings	375
UDM and HSS Range Settings	376
UDR configuration settings	377
UDR Ranges panel	377
UDR Range panel	377
UDR Nudr interface settings	378
UDR Remote SBA Nodes	380
UPF/PGW-U configuration settings	381
UPF/PGW-U Ranges panel	382
UPF/PGW-U Range panel	382
UPF N3 interface settings	383
UPF N4 interface settings	384
UPF N6 interface settings	386
UPF N9 interface settings	386
5G-EIR configuration settings	389
5G-EIR Ranges panel	389
5G-EIR Range panel	389
5G-EIR node settings	390
5G-EIR N5g-eir interface settings	390
5G-EIR Remote SBA Nodes	392
NF Discovery service	393

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	87
Node Start/Stop Rates	87
DNS Settings	88
Advanced Settings	88
DNNs panel	93
DNN configuration settings	94
Session AMBR configuration settings	97
ePCO configuration settings	98
Traffic Control Settings configuration	98
Impairment	99
QoS Flows panel	100
QoS Flow configuration settings	101
QoS Flow Max Packet Loss Rate settings	103
QoS Flow ARP configuration settings	104

QoS Flow MBR configuration settings	104
QoS Flow GBR configuration settings	105
Milenage	105
Customer Parameters	106
CA Certificates	106

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.

Setting	Description
Network Instance Format	Select the encoding format for the network instance: string or label-list. For more details, refer to Network Instance Format .
<i>Links to detailed settings:</i>	
Node Start/Stop Rates	For more details, refer to Node Start/Stop Rates .
DNS Settings	For more details, refer to DNS Settings .
Advanced Settings	For more details, refer to Advanced Settings .
DNNs	For more details, refer to DNNs .
Impairment	For more details, refer to Impairment .
QoS Flows	For more details, refer to QoS Flows .
Milenage	For more details, refer to Milenage .
Custom Parameters	For more details, refer to Custom Parameters .
CA Certificates	For more details, refer to CA Certificates .

Node Start/Stop Rates

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

Setting	Description
<i>Node Start</i>	
Rate	Set the desired start rate for SCTP connections between the NG-RAN and the AMF (connections per second).

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

DNS Settings

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

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

Advanced Settings

The following table describes the settings required to enable user plane and control plane advanced statistics.

Setting	Description
Ignore Offline Agents At Runtime	When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.
Overwrite Capture Size for IxStack	Enable this option to overwrite the capture size for IxStack.

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

Setting	Description
	and with Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.

Traffic Settings

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

Setting	Description
<i>GTPU Source Port:</i>	
Start	Indicates the source port for the GTPU tunnel. By default, the registered UDP port for GTPU is 2152.
Count	Set the count value.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable RTP.
Enable ICMP Responses	Select this option to enable it. This will permit requests and responses to ICMP packets on subscribers addresses (it will have a significant memory impact on server nodes - AMF, UPF).
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.

Response Cache

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	When this option is enabled, the server node will store the GTPv2 and PFCP Response messages for a period of time equal to Rotation Interval

Setting	Description
PFCP protocols	(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	94
Session AMBR configuration settings	97
ePCO configuration settings	98
Traffic Control Settings configuration	98

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 <code>start_value</code> (they might start with an intermediate value in the second pool).</p>
PDU Type	Select the desired PDU type: IPv4, IPv6, IPv4v6 or Ethernet.
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> .
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.
QoS Flows IDs	<p>Select the QoS Flows ID(s) from the drop-down list. Each DNN should contain at least the default flow (the default flow is unique per each DNN). In addition, zero or more dedicated flows can be associated to each DNN.</p> <p>For more details about QoS Flow configuration, refer to QoS Flow configuration settings.</p>
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) that had been allocated to the UE. SSC Mode 3: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Default SSC Mode	<p>Select the desired default SSC mode for this DNN.</p> <p>The SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session.</p>
Allowed Services	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

Setting	Description
	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	Enable this option if the UE subscription data indicates support for interworking with EPS for this DNN.
Is Local Area DN	<p>Enable 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	Enable this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.
Subscriber Spending Limits	Enable this option if the DNN will support PDU session policies that are based on subscriber spending limits.
Offline	Enable this option if the DNN will support the offline charging method for PDUs sessions.
Online	Enable this option if the DNN will support the online charging method for PDUs sessions.
Is Emergency DNN	When this option is enabled, if an UE range has mapped this type of DNN, it will perform an emergency PDU Session.
MPS Priority	Enable this option if the DNN will support subscription to MPS priority service. The priority applies to all traffic on the PDU Session.
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.
Session Rule Name	Set the session rule name.
GBR	<i>Select this option to open the GBR panel.</i>
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	<i>Select this option to open a new panel that contains the Session AMBR settings. These settings are described in Session AMBR configuration settings.</i>
ePCO	<i>Select this option to open the extended protocol configuration options panel. These settings are described in ePCO configuration settings.</i>
Traffic Control Settings	<i>Select this option to open the traffic control settings panel. These settings are described in Traffic Control Settings configuration.</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](#).
- 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.

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

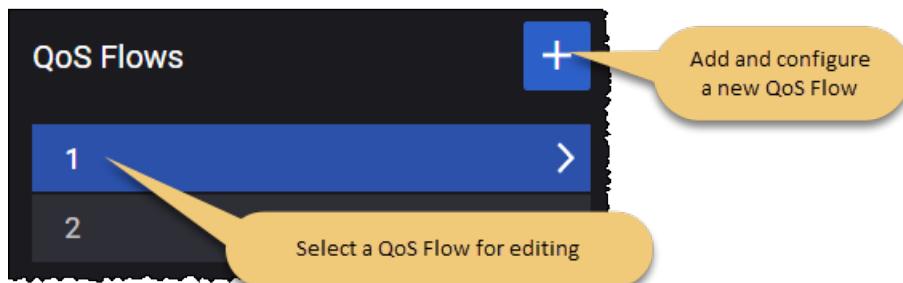
Setting	Description
Name	Each impairment profile is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Action Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Custom script • PFCP-drop message
Script file	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	101
QoS Flow Max Packet Loss Rate settings	103
QoS Flow ARP configuration settings	104
QoS Flow MBR configuration settings	104
QoS Flow GBR configuration settings	105

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	<p>Enable this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow.</p>
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	<p>Specify the 5QI value (decimal number).</p> <p>5G QoS Identifier (5QI) is a scalar that is used as a reference to 5G QoS characteristics defined in TS 23.501, clause 5.7.4. These are access node-specific parameters that control QoS forwarding treatment for the QoS Flow (such as scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, among others). Standardized 5QI values have a one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in TS 23.501, table 5.7.4-1.</p>
5QI Priority Level	Specify the 5QI Priority Level for this QoS Profile. 5QI Priority Level is a Policy Control parameter that accepts values from 1 through 127 (where 1 is the highest priority). It indicates a priority in scheduling resources among QoS Flows.
Resource	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 enabled.</p> <p>If this option is not enabled, a new Packet Filter List option appears and custom packet filter can be configured.</p>
EPS Bearer	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	If needed, enable this option.
Move to Secondary Node	If needed, enable this option. This option is part of the Option 3x and Dual Connectivity NR feature, for more details refer to UE Range Panel .
Packet Filter List	IMPORTANT This is available if Use Match-all Packet Filter option is not selected. Refer to the following topic for a description of the Packet Filter configuration settings: QoS Flow Packet Filter configuration settings .
Max Packet Loss Rate	Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: QoS Flow Maximum Packet Loss configuration settings .
ARP	Refer to the following topic for a description of the ARP configuration settings: QoS Flow ARP configuration settings .
MBR	Refer to the following topic for a description of the MBR configuration settings: QoS Flow MBR configuration settings .
GBR	Refer to the following topic for a description of the GBR configuration settings: QoS Flow GBR configuration settings .

QoS Flow 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>

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

QoS Flow MBR configuration settings

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

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

Setting	Description
<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.

Setting	Description
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set the maximum bit rate value for downlink traffic.

QoS Flow GBR configuration settings

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

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

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

Milenage

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

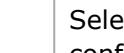
Setting	Description
R3	Set the R3 value (integer type). Default value: 32 .
C4	Set the C4 value (string type). Default value: 0004 .
R4	Set the R4 value (integer type). Default value: 64 .
C5	Set the C5 value (string type). Default value: 0008 .
R5	Set the R5 value (integer type). Default value: 96 .

Customer Parameters

The section allows you to use custom parameters. When **Use Custom Parameters** is enabled, you can use the text section below to add the custom parameters.

CA Certificates

The following table describes the settings required for CA certificates upload.

Setting	Description
<p><i>CA Certificates:</i></p>	
	Select the Add CA Certificate button to add a new certificate to your test configuration.
<p><i>CA Certificate:</i></p>	
	Select the Delete CA Certificate button to remove the certificate from your test configuration.
Name	Each certificate is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Certificate File (.crt)	It allows you to add the certificate from the storage location, using the Upload button. To remove the script, select the Clear button.

UE configuration settings



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

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

The configuration settings are described in the topics listed below.

Topics:

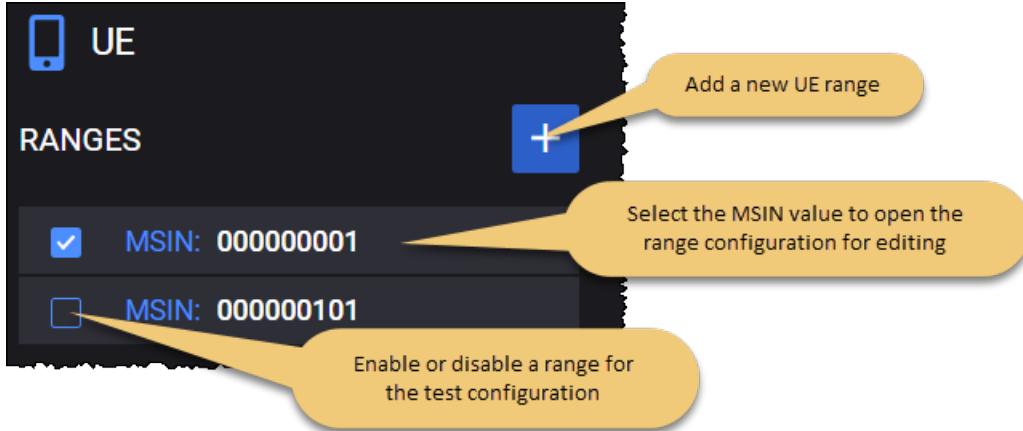
UE Ranges panel	108
UE Range panel	109
Range Settings	111
UE Identification settings	112
UE Security settings	112
UE Settings settings	116
UE Shared Data IDs	120
UE Subscribed AMBR settings	120
Service Area Restriction settings	120
Forbidden Areas	122
DNNs Config	123
Notifications	126
SMS Configuration	126
Equipment Status	127
Converged Charging	128
Spending Limit Control	129
Internal Group IDs	131
Network Slicing settings	133
UE NSSAI settings	134
UDM Default NSSAI settings	135
UDM SNSSAI Mappings	135
UDR SNSSAI Settings	136

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

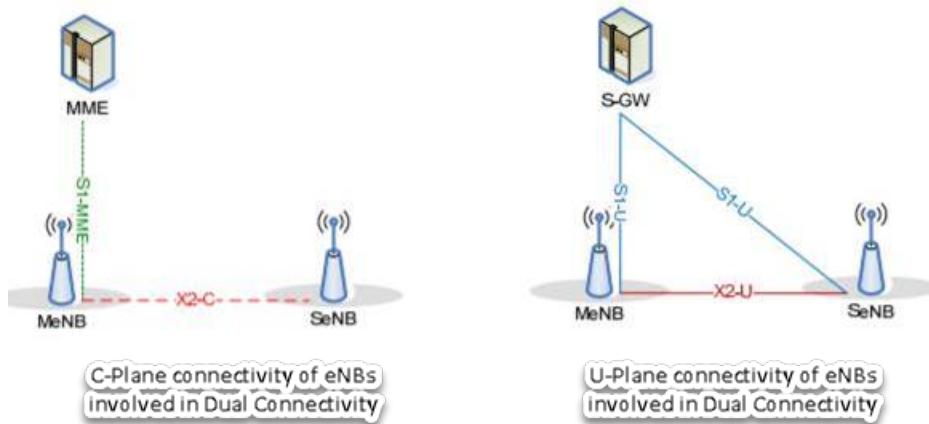
When you select an MSIN from the UE **Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- Delete the UE range from the test configuration.
- Configure the *Range Count*.
- Select the *Parent NG-RAN* for the UE range.
- Select a *Secondary Node*.
- Access the detailed UE configuration settings (Range Settings, Network Slicing, Objectives).

UE range controls and settings

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

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



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

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

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

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

Through E-RAB modification 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** [option](#) must be enabled on the QoS flows tab, on each bearer that needs to use the NR resources. The traffic will be moved to NR bearers as soon as the bearer configured to support is successfully setup.

Known limitations:

- Application Traffic is not supported on Dual Connectivity bearers.

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

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

Detailed UE configuration settings

The Range panel also provides links to the detailed configuration settings:

- [UE Range settings](#)
- [Network Slicing settings](#)
- [Test Objectives](#)

Range Settings

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

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

UE Identification settings	112
UE Security settings	112
UE Settings settings	116
UE Shared Data IDs	120
UE Subscribed AMBR settings	120
Service Area Restriction settings	120
Forbidden Areas	122
DNNs Config	123
Notifications	126
SMS Configuration	126
Equipment Status	127
Converged Charging	128
Spending Limit Control	129
Internal Group IDs	131

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

UE Security settings

Each UE range requires security settings for subscriber authentication and subscriber privacy. In the 5G system, the SUbscription Permanent Identifier (SUPI) is a globally unique identifier allocated to each subscriber. The serving network must authenticate the SUPI in the process of authentication and key agreement between UE and network. The serving network authorizes the UE through the subscription profile obtained from the home network; this UE authorization is based on the authenticated SUPI.

The SUPI is never transferred in clear text over the 5G-RAN; instead, the SUCI is used. The SUbscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed SUPI. In the 5G core network, only the UDM has authority to deconceal the SUCI.

For detailed information, refer to 3GPP TS 33.501 (Security architecture and procedures for 5G System).

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

Setting	Description						
K	<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 own choosing.</p>						
K Increment	The number used to increment the K value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same K value.						
Configure OP / OPc / TOP / TOPc	Select the operator-specific authentication value.						
OP	<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	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.						
TOP	A 256-bit operator variant algorithm configuration field used by the TUAK authentication algorithm.						
TOPc	A 256-bit value derived from TOP and K used by the TUAK authentication algorithm.						
TOPc Increment	The number used to increment the TOPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same TOPc value.						
SUCI Protection Scheme	<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" style="margin-left: 20px;"> <thead> <tr> <th>Scheme</th> <th>Identifier</th> <th>Size of the scheme output</th> </tr> </thead> <tbody> <tr> <td>null-</td> <td>0x0</td> <td>Size of the input (size of username used in case</td> </tr> </tbody> </table>	Scheme	Identifier	Size of the scheme output	null-	0x0	Size of the input (size of username used in case
Scheme	Identifier	Size of the scheme output					
null-	0x0	Size of the input (size of username used in case					

Setting	Description												
	<table border="1" data-bbox="425 255 1437 576"> <thead> <tr> <th data-bbox="434 276 556 308">Scheme</th><th data-bbox="556 276 752 308">Identifier</th><th data-bbox="752 276 1184 308">Size of the scheme output</th></tr> </thead> <tbody> <tr> <td data-bbox="434 340 556 371">scheme</td><td data-bbox="556 340 752 371"></td><td data-bbox="752 340 1437 371">of NAI format or MSIN in case of IMSI)</td></tr> <tr> <td data-bbox="434 403 556 435">Profile-A</td><td data-bbox="556 403 752 435">0x1</td><td data-bbox="752 403 1437 466">Total of 256-bit public key, 64-bit MAC, and size of input</td></tr> <tr> <td data-bbox="434 498 556 530">Profile-B</td><td data-bbox="556 498 752 530">0x2</td><td data-bbox="752 498 1437 561">Total of 264-bit public key, 64-bit MAC, and size of input.</td></tr> </tbody> </table>	Scheme	Identifier	Size of the scheme output	scheme		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											
scheme		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	<p>The Routing Indicator that is used in the construction of the SUCI.</p> <p>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.</p>												
RAND	<p>A hexadecimal number that represents the 128-bit random challenge.</p> <p>You can accept the value generated by LoadCore, or enter of a RAND value of your own choosing.</p>												
RAND Increment	Specify the RAND increment value.												
AUTN	The AUthentication TokeN (AUTN) to use when authenticating the UEs in this range.												
Authentication Type	<p>Select the Authentication Method to use in the authentication procedures for this range of UEs.</p> <p>In the current release, 5G-AKA is the only supported Authentication Type.</p>												
Integrity Protection Maximum Uplink Data Rate	<p>Select a value from the drop-down list:</p> <ul style="list-style-type: none"> • 64 kbps • Full Data Rate 												
Integrity	Select a value from the drop-down list:												

Setting	Description
Protection Maximum Downlink Data Rate	<ul style="list-style-type: none"> • 64 kbps • Full Data Rate

UDM User Plane Security Profile

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

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

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

NOTE

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

UE Settings settings

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

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

Setting	Description
	<p>a T3512 timer, which consists of a Unit-Value pair. For example, a value of 30 and unit of 10min means 300 minutes.</p> <p>The T3512 timer can be overridden by subsequent Registration Accept messages. If T3512 is 0 or Disabled, no periodic registration should be performed. If no T3512 value is present in the Registration Accept message, the last known T3512 value is used. If a T3512 was never transmitted by the AMF, the default value of 54 minutes will be used.</p> <p>The T3512 timer is triggered when the UE enters idle. If the UE exits the idle state, the T3512 timer is stopped. When the UE enters again in idle, the T3512 timer is restarted.</p> <p>While the UE is in idle mode, when the T3512 timer expires:</p> <ul style="list-style-type: none"> • If the UE is not registered for emergency services, the UE initiates a Periodic Registration Update procedure and restarts the T3512 timer. • If the UE is registered for emergency services, the UE locally de-registers and the AMF locally de-registers the UE.
Delay Before PDU Session Creation (ms)	The time that will elapse before the UEs in this range begin creating PDU sessions after successful Registration.
Delay Before Deregister (ms)	The time that will elapse between PDU Session Release Complete and UE initiated Deregistration Request messages.
Delay Before Handover Notify (ms)	The time to wait before handover notification.
Delay Before Paging (ms)	The time to wait before paging, after UE enters idle.
Check AUTN	<p>By default, this option is disabled.</p> <p>When the option is enabled, then UE will check the value of AUTN in the <i>Authentication Request</i> messages and it will reply with <i>Authentication Failure (MAC failure)</i> in case of different MAC values or with <i>Authentication Failure (Synch failure)</i> in the case the sequence number computed using the AUTN value is invalid.</p>
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.
Always Include Uplink Data Status IE in Service Request Message	The UE will always include the Uplink Data Status IE for a Service Request message, not only if it has pending data.
Enable Passthrough	Select this option to enable passthrough and any interface.

Setting	Description
	<p>Applicable to all passthrough topologies (UE/gNB or UPF).</p> <p>Applicable to either direction: GTPu to IP or/and IP to GTPu.</p>
Attach/Register with GUTI	When the Primary Objective type is Subscribers Per Second, enabling this option will trigger a Registration/Attach Request with the type of user identity set to temporary identity (GUTI). When option is not enabled, the type of user identity in the Registration/Attach Request will be permanent identity.
Force Emergency Registration	<p>When this option is enabled, the UE will perform an Emergency registration (instead of Initial Registration).</p> <p>Only the primary objective's DNNs are taken into account when deciding if the UE performs an emergency registration. When the <code>dnnIdsToActivate</code> is present but empty in the primary objective, the Emergency Registration will not be performed even if there is a Secondary Objective that uses an emergency DNN.</p>
Identity Type for Emergency Registration	Select an option from the drop-down list. Available options: SUCI or IMEISV .
Support SMS	<p>When this is selected, a flag will be added in the Registration message advertising UE support for SMS over NAS feature.</p> <p>This feature is currently available on gNB N1N2 interface but not on the Full Core AMF, so the AMF needs to be set as DUT.</p>
Delay Before Indirect Forwarding Cleanup (ms)	The time that will elapse before indirect forwarding cleanup. The delay is calculated from the UE Context Release.
Send Native GUTI During IRAT Mobility Registration	Enable this option to send native GUTI during IRAT mobility registration.
Authentication During Mobility Registration	<p>Select a value from the drop-down list:</p> <ul style="list-style-type: none"> • Never: Authentication is not performed during mobility registration. • Always: Authentication during mobility registration is always performed. • No Native Context: Authentication during mobility registration is performed only when the UE does not hold a native 5G security context.
<i>Access and Mobility Policy:</i>	
Subscription Categories	<p>Select the desired Subscription Category for this range of UEs.</p> <p><i>Subscriber Category</i> is an information type structured as a list of category identifiers associated with a subscriber. It may comprise any</p>

Setting	Description
	<p>number of identifiers associated with the subscriber (such as platinum, gold, silver, bronze).</p> <p>Applicable to simulated UDR NF.</p>
<i>Radio Capability</i>	
UE Radio Capability IE Value for LTE	The UE radio capability IE value that will be included UE Capability Info Indication message.
UE Radio Capability IE Value for NR	The UE radio capability IE value that will be included UE Capability Info Indication message.
Send UE Capability IE Indication after Initial Context Setup	Select this option to sent UE capability IE indication after initial context setup.
<i>Location Reporting</i>	<p>Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).</p>
Reporting Type	<p>Select the value from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • Direct - If the test timeline is long enough, the AMF generates n LocationReportingControl messages at every m seconds from the moment Registration Complete message is received by the AMF (n is the value configured for Number of Repeats and m is the value of Interval Between Requests). • Change of Serving Cell - In case of Handover with AMF change, if Change of Serving Cell is selected, after handover, the new AMF will send a LocationReportingControl message to the NG-RAN.
Interval Between Requests (seconds)	Set the time interval between requests.
Number of Repeats	Set the number of repeats.
Start Time (seconds)	The number of seconds after successful attach when the AMF sends a LocationReportingControl message (event-type: change-of-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.

Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.

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

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.

Use the settings described below to configure service area restrictions for a UE range. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.

Service Area Restrictions

Setting	Description
Restriction Type	The type of restriction to use for this range of UEs. It is either Not Allowed Areas or Allowed Areas .

Setting	Description
	<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 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.

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>

DNNs Config

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

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

Setting	Description
<i>DNNs Config:</i>	
	From the panel, you can select a DNN Config for editing and also add additional DNN configurations. Select the Add DNNs Config button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the Delete DNN Config button to delete this DNN config from your test configuration.
SSC Mode	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) that had been allocated to the UE. SSC Mode 3: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Session ID	Provide the session ID value.
Reactivation Delay(s)	<p>This per DNN timer defines the interval between the moment a User Plane connection of an existing PDU Session was deactivated by the network and the moment the UE reactivates it (via Service Request). For more details, refer to TS 23502 4.2.3.2.</p> <p>This timer is applied only if the User Plane connection of an existing PDU Session was previously deactivated. Otherwise, it is ignored.</p> <p>The default value of 0 means no reactivation.</p> <p>NOTE The reactivation delay is deactivated if an IRAT mobility occurs before the timer expires.</p>
DNN	Select one of the previously-defined DNNs from the drop-down list.

Setting	Description
Local IPv4 Address	<p>The IPv4 address that the UE receives from the SMF during PDU Session Establishment. This address is used for L4-7 traffic (source IP for the UL traffic, destination IP for the DL traffic). It is used only when LoadCoresimulates the SMF.</p> <p>IP address is also used to create UE Routes from DN.</p>
Local IPv4 Prefix Length	<p>The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.</p>
Local IPv6 Address	<p>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 LoadCoresimulates the SMF.</p> <p>IP address is also used to create UE Routes from DN.</p>
Local IPv6 Prefix Length	<p>The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.</p>
Ethernet Device Information	<p>Allows adding multiple ethernet devices per DNN with PDU type Ethernet.</p> <p>NOTE This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</p>
Ethernet PDU config	<p>For each ethernet device the MAC Address, IP Address, outer VLAN and inner VLAN can be configured.</p>
Enable TSN	<p>This feature is available only for spec version newer (including) Release 16 and Ethernet PDU type sessions.</p> <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	<p>The device-side TSN translator port MAC address.</p>
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 from Allowed NSSAI list (received in Registration Accept) 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	<p>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.</p>
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

Setting	Description
	<p>Session Establishment message (as the slice selected from the above list is not part of Allowed NSSAI).</p> <ul style="list-style-type: none"> 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>
<i>Secondary Authentication:</i>	
Method type	<p>The following options are available:</p> <ul style="list-style-type: none"> None EAP-TTLS (Extensible Authentication Protocol – Tunnelled Transport Layer Security) CHAP (Challenge-Handshake Authentication Protocol) PAP (password Authentication Protocol)
<i>EAP-TTLS Auth Method:</i>	
Client Certificate	Provide the client certificate.
Tunneled Authentication Method	Select the tunneled authentication method: <ul style="list-style-type: none"> PAP CHAP
Password	Provide the password.
Send User Identity	<p>By default, this option is disabled.</p> <p>Enabling this option will add SM PDU DN Request Container IE (Authentication Identity) to the PDU Session Establishment Request message send by NG-RAN.</p>
<i>Chap Auth Method:</i>	
User	Provide the user.
Secret	Provide the password.
<i>PAP Auth Method:</i>	
User	Provide the user.
Password	Provide the password.

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 (ms)	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 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	The type of number can be one of the following: <ul style="list-style-type: none"> • Unknown • International number • National number • Network specific number • Subscriber number • Alphanumeric • Abbreviated number

Setting	Description
	<ul style="list-style-type: none"> • Reserved number
Numbering Plan Identification	The numbering plan identification can be one of the following: <ul style="list-style-type: none"> • Unknown • ISDN • Data numbering plan • Telex numbering plan • National numbering plan • Private numbering plan • ERMES numbering plan • 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.
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 Termintated. The UE range waits for delivery of SMS messages.

Equipment Status

The Equipment Status lets user configure blocked or greylisted ranges of UEs using the IMEI. Applicable to simulated 5G-EIR Network Function.

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.

Setting	Description
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.

Converged Charging

Applicable to simulated CHF Network Function. The following table describes the UE **Converged Charging** settings.

Setting	Description
Validity Time	The validity of the granted quota for a given category instance.
Quota Holding Time	A quota expiry time, when no traffic associated with the quota is observed for the value indicated by this attribute.
Time Quota Threshold	A time quota below this threshold will trigger a quota re-authorization.
Volume Quota Threshold	A volume quota below this threshold will trigger a quota re-authorization.
Unit Quota Threshold	A units quota below this threshold will trigger a quota re-authorization.
Notification Timer	Duration in milliseconds after which the CHF will notify CTF about quota re-authorization.
Enable Subscription Termination Timer	Select this option to enable the subscription termination timer.
Trigger Subscription Termination (ms)	Set the value for this parameter.
<i>Total Available Units Per PDU Session:</i>	<i>Holds the maximum amount of units to be granted per PDU session per charging session.</i>

Setting	Description
Total Time	Set the total time value.
Total Volume	Set the total volume value.
Total Uplink Volume	Set the total uplink volume value.
Total Downlink Volume	Set the total downlink volume value.
Total Service Specified Units	Set the total service specified units value.
<i>Default Granted Units Per Charging Data Request:</i>	
Time	Set the time value.
Volume	Set the volume value.
Uplink Volume	Set the uplink volume value.
Downlink Volume	Set the downlink volume value.
Service Specified Units	Set the service specified units value.

Spending Limit Control

Applicable to simulated CHF Network Function. The following table describes the UE **Spending Limit Control** settings.

Setting	Description
Enable Notify Timer	Use this option to enable 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	Use this option to enable 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	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.
Policy	<i>These settings are described here.</i>

Setting	Description
Counters	
Notify Policy Counters	These settings are described here .

Policy Counters

Applicable to simulated CHF Network Function. 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.
<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 Counter Status	Enter the policy counter status (as a string value). For example: <i>120Mbps</i> .
Activation Time	Enter the activation time (as a DateTime value) for this status value. For example: <i>2020-12-31 11:59:59</i> .

Internal Group IDs

Applicable to simulated UDM Network Function. The following table describes the **UE Internal Group IDs** settings.

Setting	Description
	Select the Add Internal Group ID button to add a new internal group to your test configuration.
<i>Internal Group ID Info:</i>	
	Select the Delete Internal Group ID button to delete this group from your test

Setting	Description
	configuration.
Internal Group ID	This parameter is used to identify an internal group. You can accept the value provided by LoadCore or overwrite it with your own value.
External Group ID	This parameter is used to identify an external group.
Shared Data ID	Select the shared data ID from the drop-down list.
DNN Name	Select the Data Network Name (DNN) value from the drop-down list.
S-NSSAI	Select the S-NSSAI slice from the drop-down list.

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	134
UDM Default NSSAI settings	135
UDM SNSSAI Mappings	135
UDR SNSSAI Settings	136

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 NSSAI slices are the ones supported and requested 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 **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 configured 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>	

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

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.

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	138
About primary objectives	139
Primary Control Plane Objective	141
Secondary Control Plane Objective	143
User Plane Objectives	153
Stateless UDP Traffic	154
Data Traffic	155
Voice Traffic	159
Video OTT Traffic	173
DNS Client Traffic	176
ICMP Client	179
Ping Traffic	180
Capture Replay	181
Predefined Applications Traffic	183

Control Plane Objective

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

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

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

About primary objectives

In the current 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](#)
- [Subscribers Per Second](#)

Active Subscribers

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

<i>Ramp Up Time:</i>	20000 / 1000 = 20s for subscribers to register
<i>Rate in ramp up time:</i>	1000 registrations per second

<i>Sustain time:</i>	30 seconds
<i>Rate in sustain time:</i>	2000 secondary procedures per second
<i>Ramp down time:</i>	$20000 / 1000 = 20\text{s}$ 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 after NG-Setup/S1-Setup have successfully completed.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p> <p>You configure DNNs for the test in the Global Settings. Refer to DNNs panel for more information.</p>
Number of Retries	This value indicates how many times UE/NGRAN will retry the Register or PDU Session Establishment procedures if any message from these procedures encounters an error (timeout or an error is received).

Parameter	Description
	<p>The available options are:</p> <ul style="list-style-type: none"> • -1 : infinite retries for entire sustain time. • 0 (default value) : the retry option is disabled. • 1 to 127: the number of retries per UE (Register + PDU Session procedure).
<i>Subscribers Per Second:</i>	
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.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p> <p>You configure DNNs for the test in the Global Settings. Refer to DNNs panel for more information.</p>

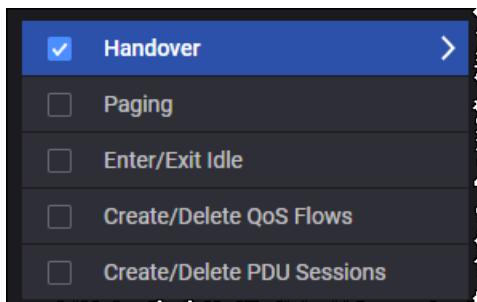
Secondary Control Plane Objective

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

Handover

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

Handover 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.
- X2 handover and S1 handover are supported in Connected mode on RAN only (not supported in Idle mode or 4G FullCore topology).
- X2 handover is executed when the MME serving the UE can reach the target RAN (T-RAN) and an X2 link is configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.

S1/N2 handover scenarios

For S1/N2 handover there are the following scenarios:

Scenario	Description
S1/N2 handover with MME/AMF change and Direct Forwarding	This scenario is executed when the MME/AMF serving the UE cannot reach the target RAN (T-RAN) and an X2/Xn link is configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.
S1/N2 handover with MME/AMF change and Indirect Forwarding	This scenario is executed when the MME/AMF serving the UE cannot reach the target RAN (T-RAN) and an X2/Xn link is not configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.
S1/N2 handover without MME/AMF change and Indirect Forwarding	This scenario is executed when the MME/AMF serving the UE can reach the target RAN (T-RAN) but an X2/Xn link is not configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.
S1/N2 handover without MME/AMF change and Direct Forwarding	This scenario is executed when the MME/AMF serving the UE can reach the target RAN (T-RAN), Force S1 / N2 Handover option is set and X2/Xn link is configured between the source RAN (S-RAN) and the target RAN (T-RAN) in the Ranges Connectivity matrix.

Option 3x handover scenarios

In S1-MME RAN simulation scenarios, for Option 3x 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

In 4G Full Core simulation scenarios, for Option 3x handover there is support for the following:

- Add / Remove Secondary node as long as the Master Node remains the same (no support for 4G FullCore X2 handover).

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.

Dual Connectivity NR-NR handover scenarios

In N2N3 RAN simulation scenarios, for Dual Connectivity NR-NR handover there is support for the following:

- Xn Handover support between gNodeBs – only N2 signaling is visible
- Dual Connectivity NR-NR handovers support:
 - Inter-Master Node handover with/without Secondary Node change (Xn handover between 2 gNodeBs that have a Secondary Node configured)
 - Master Node to gNodeB Change (Xn handover from a gNodeB with SN node to one without a SN configured)
 - gNodeB to Master Node

Known limitations:

- Dual Connectivity NR-NR is supported only on Wireless Core SIM and Wireless NG-RAN Simulation topologies.
- Only Xn Handovers are supported to and from gNodeBs configured with Secondary Nodes.
- iRAT and N2 Handovers are not supported with Dual Connectivity NR feature.
- Enter/Exit Idle and Paging objectives are not supported Dual Connectivity NR feature.

Handover configuration parameters

The following table describes these objective parameters.

Parameter	Description
<i>Handover:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which handovers are initiated, measured in procedures per second if Distributed over (s) is not modified.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Force S1 / N2 Handover	Enable this option to force S1 / N2 handover with direct forwarding instead of X2 / Xn handover.
Mobility for State	This option specifies in what state should the UE perform the handover objective. The following options can be selected from the drop-down list: <ul style="list-style-type: none"> • Connected • Idle • Any When Any is selected, the UE will execute the handover objective, regardless if the UE is in Connected or Idle state.
Force UE State Before Returning to Parent Node	Select an option from the drop down list: <ul style="list-style-type: none"> • None - The UE will perform either Idle Mode Mobility or Connected Handover to parent RAN, depending on what state the UE is before executing the procedure. • Connected - The UE will perform Connected Handover from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in idle state before performing this mobility, the UE will first perform exit idle, and only after the UE is in connected state, will it initiate the connected handover to the parent RAN. • Idle - The UE will perform Idle Mode Mobility from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in connected state before performing this mobility, the UE will first

Parameter	Description
	perform enter idle , and only after the UE is in idle state, will it initiate the idle mode mobility to the parent RAN.
<i>Visited gNodeBs/eNodeBs : A list of the NG-RANs that UEs will visit during the test.</i>	
	Add next node to the list.
	Remove the selected node from the list.
Force UE State before Mobility	The following options can be selected from the drop-down list: <ul style="list-style-type: none"> • Connected • Idle • Any
Primary Node	Select the primary node from the drop-down list.
Secondary Node	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>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.

Parameter	Description
Suspend Traffic Interval (s)	The time (in seconds) to suspend traffic on the remote IP address.
Remote IP Address	Set the remote IP address: <ul style="list-style-type: none"> If the UPF is the DUT in the test topology, then set the <i>Remote IP Address</i> to the DN IP address. If the UPF is simulated in the test topology, then set the <i>Remote IP Address</i> to the N3 IP address of the UPF.

Notes:

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

Enter/Exit Idle

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

NOTE

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

The following table describes the objective parameters.

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

Parameter	Description
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	The number of seconds to wait between each successive state transition.

Create/Delete QoS Flows

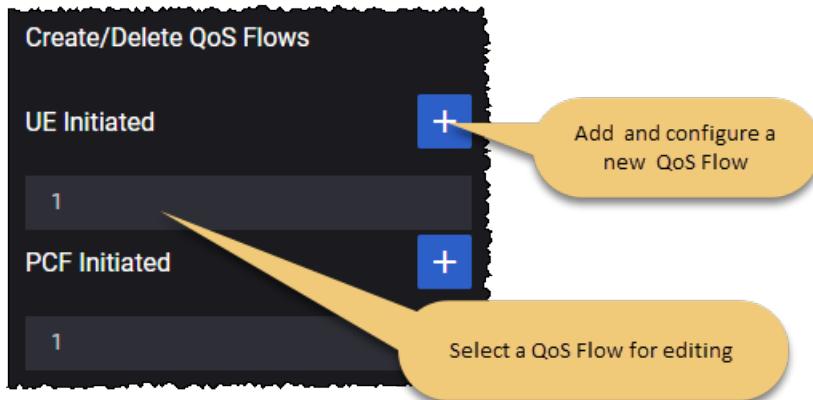
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured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

QoS flow options

There are two options for creating QoS flows:

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

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



Objective parameters

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

Parameter	Description
<i>Create/Delete QoS Flows:</i>	
	Select the Add Objective button to add an instance of this objective.
<i>Objective:</i>	
	Select the Delete Objective button to delete this Secondary Objective from your

Parameter	Description
	test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameters requires a large number of UEs configured in the test in order to achieve the desired rate.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	Interval between the triggering of creation and deletion of the QoS flow, in seconds.
DNN	Select the DNN value for the drop-down list. For example: dnn.keysight.com.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

Support for Network Initiated QoS Flow modification

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

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

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

Notes:

- In order to modify the default QoS flow, it needs to be configured on the DNN tab. The QoS Flows and DNNs are configured in the Global Settings.
- None of the parameters changed by the network initiated QoS flow modification will be enforced.

- The NG-RAN node supports handling the QoS flow modification procedure only for one PDU session per procedure (Create QoS Flow, Modify QoS Flow, Release QoS Flow).
- For UE Initiated dedicated QoS Flows, the interval between the creation and deletion of the QoS flow should be large enough to support the successful finalization for the modification of the existing QoS flow. (*Interval* is one of the Objective settings.)

Create/Delete PDU Sessions

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

The following table describes the objective parameters.

Parameter	Description
<i>Create/Delete PDU Sessions:</i>	
	Select the Add Objective button to add an instance of this objective.
<i>Objective:</i>	
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameter requires a large number of UEs configured in the test in order to achieve the desired rate.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	The interval between the triggering of creation and deletion of the PDU Session, in seconds.
DNNs to Activate	Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the DNNs Config Range settings.) The choices are:

Parameter	Description
	<ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list. <p>The list of available DNNs include those that have not been activated for the primary objective.</p> <p>You configure DNNs for the selected UE in the DNNs Config Range settings. The list of available DNNs include those that have not been activated for the primary objective.</p>

SMS

This objective will perform the procedure of sending SMS messages.

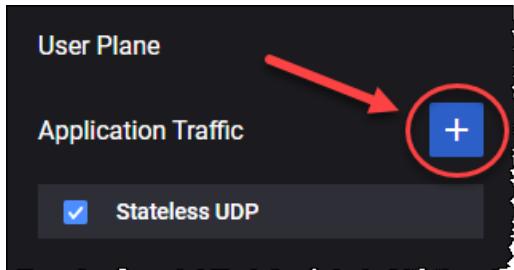
The following table describes the objective parameters.

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

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

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

The following table describes the Stateless UDP parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Flow Type	This field is set to uplink and can not be modified since on the UE you can only configure the uplink flow.
Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.
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.

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

Data Traffic

The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Throughput . The other options are: Concurrent Connections and Connections Rate .
Concurrent Connections	<p>Set the number of concurrent connections.</p> <p>This parameter is available only when Objective type is set to Concurrent Connections.</p>
Connection Duration (s)	<p>Set a value for the connection duration.</p> <p>This parameter is available only when Objective type is set to Concurrent Connections.</p>
Connections Rate per Second	<p>Set the value for connections rate per second.</p> <p>This parameter is available only when Objective type is set to Connections Rate.</p>

Parameter	Description
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
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 for a description of the configuration settings for these traffic flows. Also, you can add custom parameters, based on your test configuration requirements.</p>

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> If Optimize Throughput (per UE) option is enabled: TCP, TLS, QUIC or UDP. If Optimize Throughput (per UE) option is disabled: TCP, TLS or UDP.
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get, HTTP Put, HTTP Post and FTP. For TLS transport protocol: HTTPS Get, HTTPS Put and HTTPS Post. For QUIC transport protocol: HTTP3 Get, HTTP3 Put and HTTP3 Post. For UDP transport protocol: UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket) <div style="background-color: #e0e0e0; padding: 5px; margin-left: 20px;"> NOTE UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receives the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds. </div>
Port	The port used by the flow.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.

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

Custom Parameters

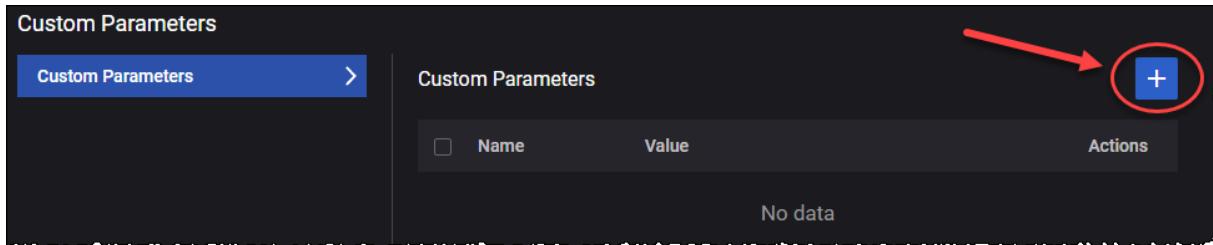
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

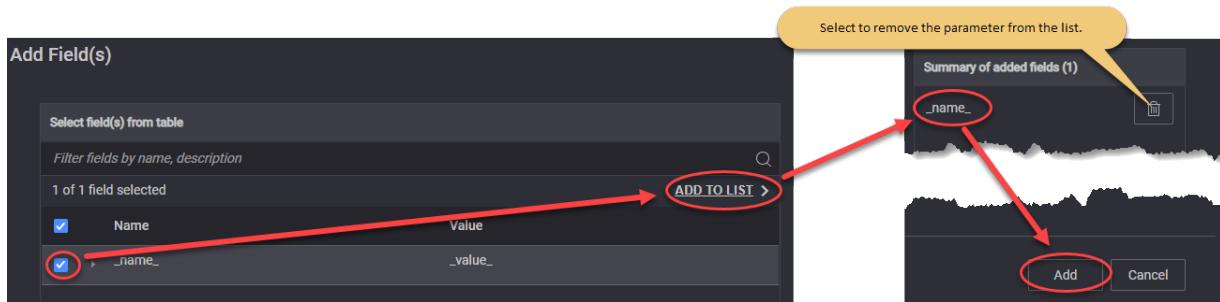
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Call Type	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.

Parameter	Description
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security • UDP - User Datagram Protocol
Enable IPSEC	Select this option to enable IPSEC.
Domain	Provide the domain name.
Advanced SIP Settings	For more details about these settings, refer to Advanced SIP Settings .
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select this option in order to enable RTCP.
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
DNN ID	Select the DNN from the drop-down list.
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
UPDATE	Select this button in order to update IMSI and Source Phone with UE range identification settings.
IMSI	Read-only field, it displays the updated IMSI.
IMSI Phone Increment	The value by which the IMSI phone number is incremented.
Destination Phone	The destination phone number.
Destination Phone	The value by which the destination phone number is incremented.

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

Media Settings

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

Parameter	Description
Media Duration (ms)	Length of time to play the media 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	Select the audio codec from the drop-down list. The available options are: <ul style="list-style-type: none"> • AMR - The Adaptive Multi-Rate (AMR) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • AMR-WB - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data 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

Parameter	Description
	<p>EVS AMR-WB IO mode for interoperability with AMR WB devices.</p> <ul style="list-style-type: none"> • PCMU • PCMA • iLBC • G722 • G723 • G729 <p>The parameters of each audio codec are presented below.</p>
<i>Advanced Media Settings</i>	
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	<p>Select the template from the drop-down list:</p> <ul style="list-style-type: none"> • None • EVS/AMR IPv4 • NB Codecs IPv6 • AMR-WB IPv6 • Multimedia IPv4

AMR/AMR-WB

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

Parameter	Description
	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.

Advanced SIP Settings

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

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

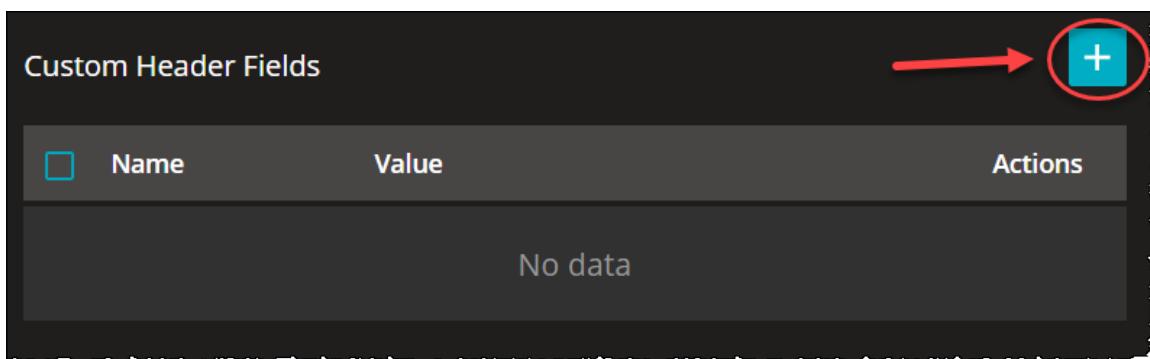
SIP Custom Headers

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

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

For each message, you can:

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



The Add Field(s) opens.

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

The screenshot shows the "Add Field(s)" dialog. On the left is a table with columns "Name" and "Value". One row for "Accept-Encoding" has its checkbox checked and is highlighted with a red circle. An arrow points from this row to a blue button labeled "ADD TO LIST". Another arrow points from this button to a summary box on the right. The summary box is titled "Summary of added fields (1)" and lists "Accept-Encoding". A yellow callout bubble above the summary box says "Select to remove the field from the list." At the bottom of the dialog are "Add" and "CANCEL" buttons.

The following custom header are available:

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

Parameter	Description	Value
Accept-Language	IETF RFC 3261	da, en-gb;q=0.8, en;q=0.7
Alert-Info	IETF RFC 3261	:<urn:alert:service:call-waiting>
Allow	IETF RFC 3261	INVITE, ACK, UPDATE, PRACK, CANCEL, PUBLISH, MESSAGE, OPTIONS, SUBSCRIBE, NOTIFY
Allow-Events	IETF RFC 6665	conference
Authentication-Info	IETF RFC 3261, IETF RFC 3310	nextnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	< http://www.example.com/alice/photo.jpg > ;purpose=icon
Content-Disposition	IETF RFC 3261	session
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:00 GMT	IETF RFC 3261

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

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

Parameter	Description	Value
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=False,algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>,<sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org?Replaces=425928%40bobster.example.com.3%3Btag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC	proxy

Parameter	Description	Value
on		3841
Require	IETF RFC 3261	Path
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-	IETF RFC	active

Parameter	Description	Value
State	6665	
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

SIP Authentication

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

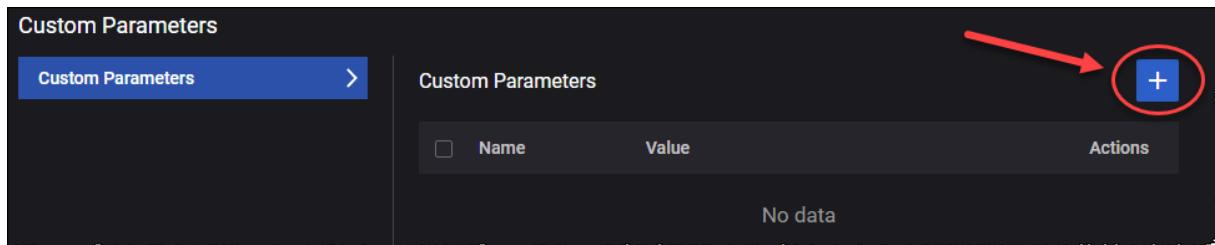
Parameter	Description
Username	Provide the username.
Password	Provide the password.
Authentication Type	Select the authentication type: <ul style="list-style-type: none"> • Digest MD5 • AKAv1 • AKAv2 • ProxyDefined
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber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

Parameter	Description
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.

Custom Parameters

You can add custom parameters as follows:

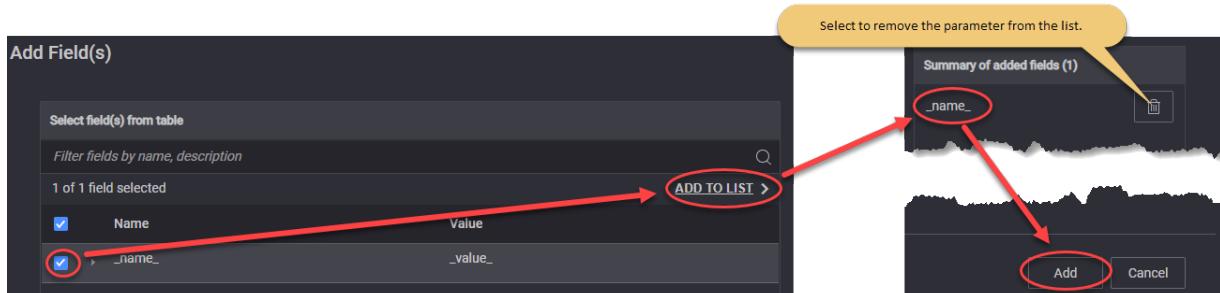
1. The Custom Parameters panel, select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom parameters are available:

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

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

SIP 3GPP IPSEC

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

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

Video OTT Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	Select the value from the drop-down list: Simulated Users or Throughput .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
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.
Flow:	

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

Quality Control

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

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

Parameter	Description
MOS P.1203	Select an option from the drop-down list: Disabled or Mode 0 .
.Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> • Adaptive Bit Rate • Quality Predefined Levels • Lowest Quality • Highest Quality
Number of segments	This field is available and editable only when the Quality Control Mode is set to Adaptive Bit Rate .
<i>Play Profiles: The following settings are available and editable only when the Quality Control Mode is set to Quality Predefined Levels.</i>	
	Select this button to add a predefined play profile to your test configuration.
<i>Quality Shift</i>	
	Select this button to remove this play profile from your test configuration.
Shift Type	Select the shift type from the drop-down list. Available options <ul style="list-style-type: none"> • Stay at Current Bitrate • Change to the Lowest Bitrate • Change to the Lowest Bitrate • Change to the Lower Bitrate • Change to the Higher Bitrate
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to Change to Higher Bitrate or Change to Lower Bitrate .
Play Until End	If this check box is selected, the Play duration field is disabled and the original playtime is used.
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.

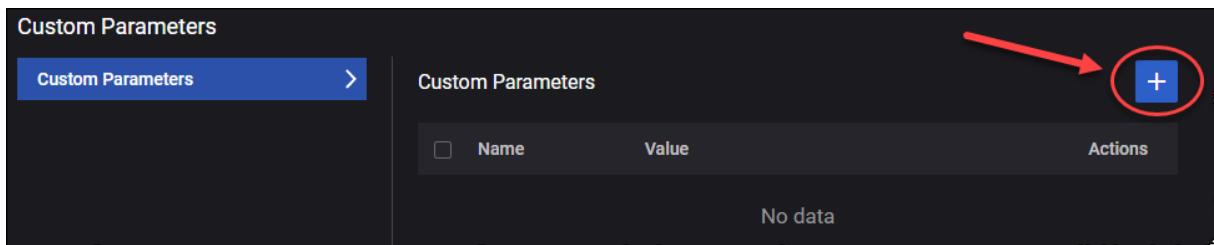
Parameter	Description
DNN ID	Select the DNN from the drop-down list.

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

Custom Parameters

You can add custom parameters as follows:

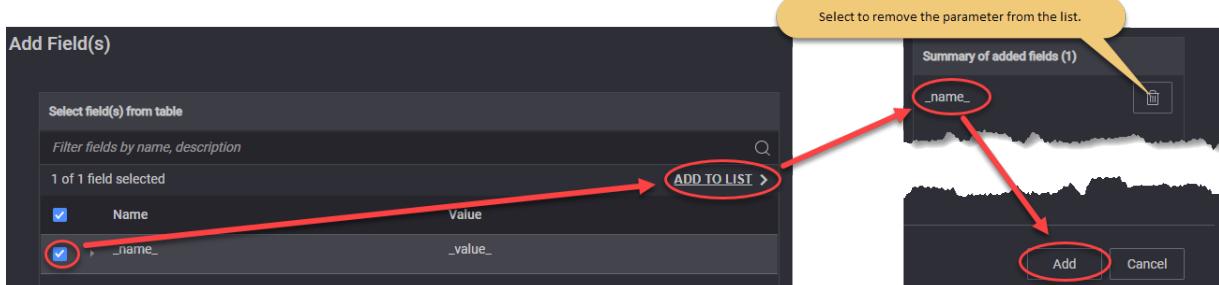
1. Select the **Open Custom Parameters** tile. The Custom Parameters panel opens.
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DNS Client Traffic

The following table describes the DNS Client Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to DNS Client .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.

Parameter	Description
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Connection multiplier (per UE)	Set the value for the connection multiplier.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select 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 Flow for a description of the configuration settings for these traffic flows. Also, you can add custom parameters , based on your test configuration requirements.

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Type	By default, the type is set to DNS Client .
Port	The port used by the flow.
DNS Server IP	Set the DNS server IP address.
Number of DNS servers	Set the number of DNS servers.
Hostname	Set the hostname.
Query Type	Select the query type from the drop-down list. The available options are: <ul style="list-style-type: none"> • A • AAAA • CNAME • TXT • PTR • NS
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Config).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

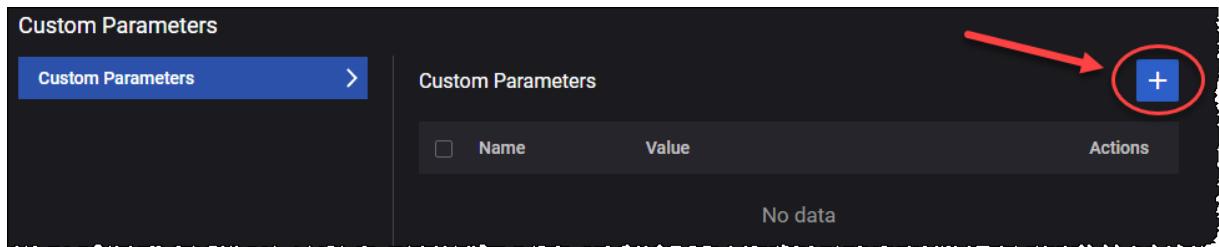
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

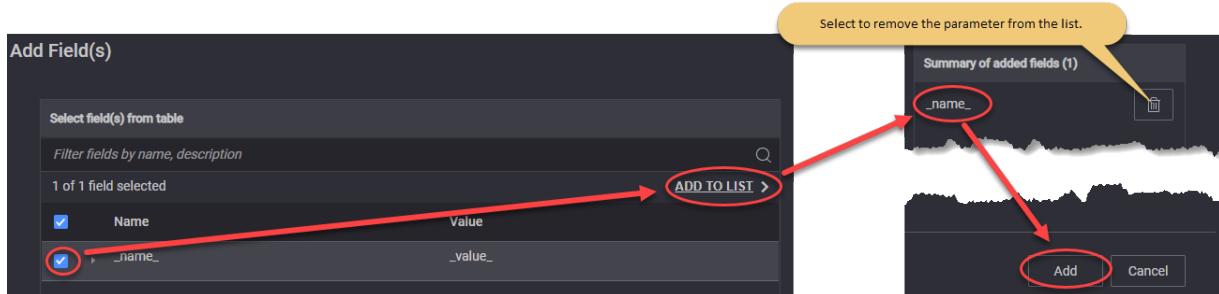
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



ICMP Client

The following table describes the ICMP Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to ICMP Client .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Traffic Flow	Refer to Traffic Flow for a description of the configuration settings for these traffic flows.

Traffic Flow

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

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

Ping Traffic

This application traffic type emulates a PING client.

The following table describes the Ping Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
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.
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.
Count	Set the count value. Default value: 4.
Interval (ms)	Set the interval value. Default value: 1000.
Timeout (ms)	Set the timeout value. Default value: 4000.

Parameter	Description
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range settings (DNNs Config).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .

Capture Replay

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

The following table describes the Capture Replay parameters.

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

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

The following table describes the Filter object parameters.

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

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

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 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,</p>

Parameter	Description
	unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
Configure Traffic Profiles	Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions. Refer to Traffic Profile for a description of the configuration settings for these traffic profiles.

Traffic Profile

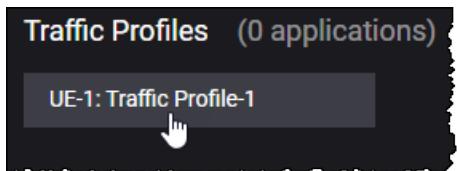
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

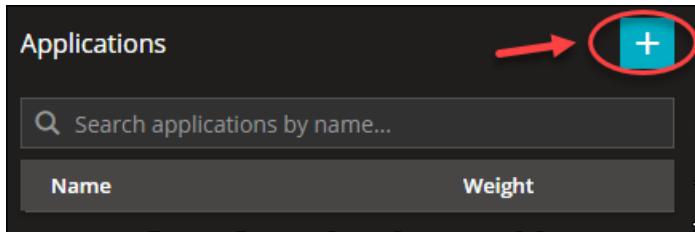
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

Applications

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

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



The Add Application(s) window opens.

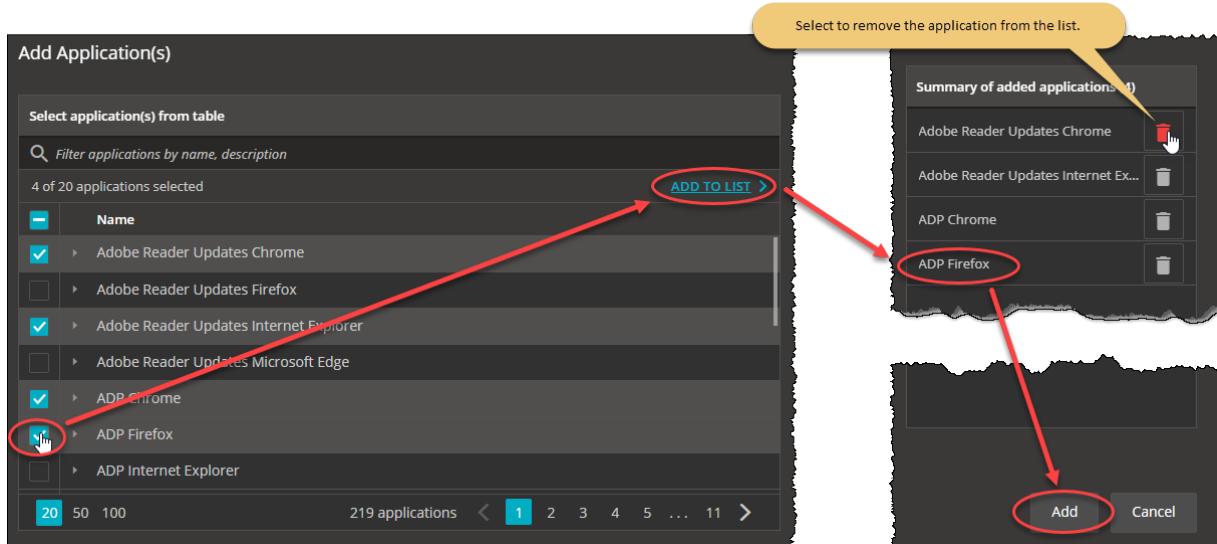
2. From the Add Application(s), select the applications you want to add and select **ADD TO LIST** to move them to the added applications section. To add the applications to your configuration select **Add**.

NOTE

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

Each predefined application flow will consume 1 WRLS-5GC-UPFLOW license feature.

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's a search bar and a table listing applications with columns for Name and Weight. One row is selected, showing 'Adobe Reader Updates Chrome 1' with a weight of 1. On the right, there are two main sections: 'Application Settings' and 'Application Actions'. The 'Application Settings' section contains fields for Destination Hostname, DNN ID, and QoS Flow ID. The 'Application Actions' section contains a search bar and a table listing actions with columns for # and Name, showing 'Check For Updates' and 'Download Updates'.

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.

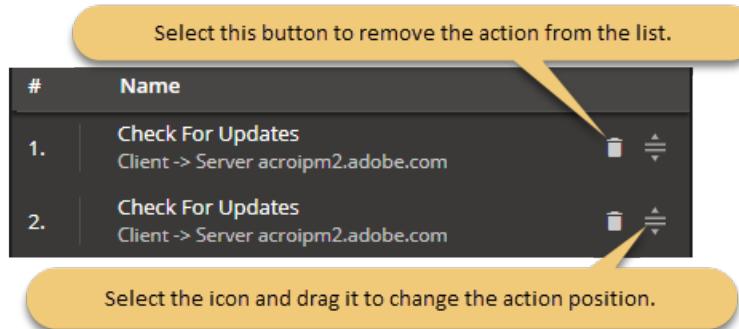
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

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:

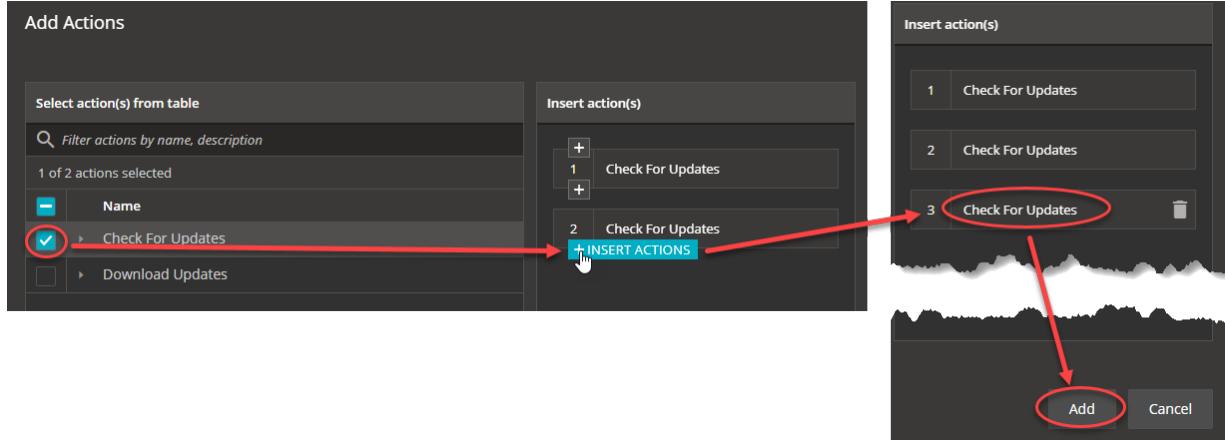
1. Use the icons available for each icon in order to remove it or to change its position in actions list.
For example ...



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 ...



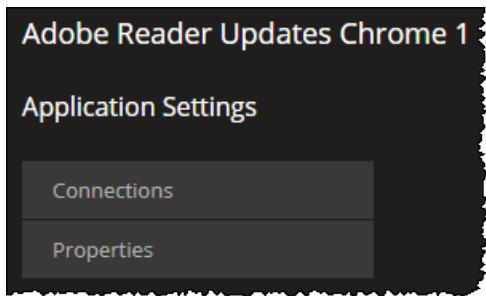
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

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.

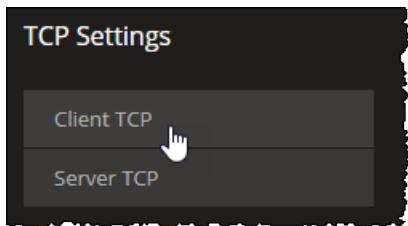
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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.



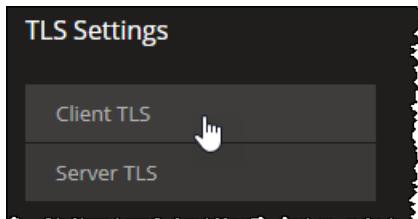
These parameters are configurable for both Client and Server settings, as presented in the following table.

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 style="text-align: center;">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.
SNI Enabled	<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.
Certificate file	<i>Select Upload to add your certificate file or Clear to remove it.</i>
Key file	<i>Select Upload to add your key file or Clear to remove it.</i>
Key file password	<i>Enter your key file password.</i>
DH file Traffic	<i>Select Upload to add your DH file or Clear to remove it.</i>

RTP Settings

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

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

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	195
AMF Range settings	196
AMF node settings	197
AMF N2 interface settings	200
AMF Namf interface settings	201
AMF N26 Interface Settings	202
AMF remote SBA nodes	203

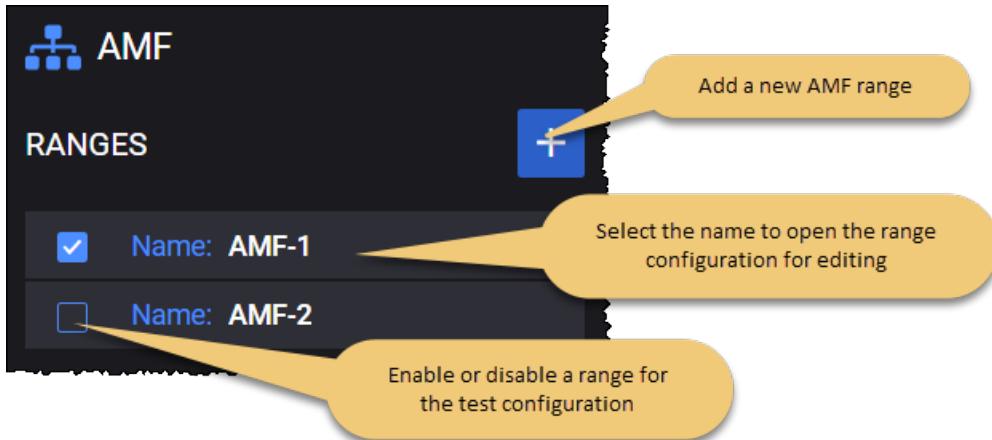
AMF Ranges panel

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 .
N2 Interface Settings	Each AMF range requires the configuration of N2 interface settings, through which a AMF instance interacts with RAN in a 5G network. These settings are described in AMF N2 interface settings .
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 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 .
Remote SBA Nodes	These settings are described in AMF remote SBA nodes .

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.
Relative Capacity	Set the relative capacity value.
Ciphering Algorithm	Allows to select the supported 5G ciphering algorithm: <ul style="list-style-type: none"> NEA0 - Null ciphering algorithm NEA1 - 128-bit SNOW 3G based algorithm NEA2 - 128-bit AES based algorithm
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	Enable this option to request N2 SM Information again instead of using the existing one.
Establish UE Policy Association	Enable this option to trigger Establishment of UE Policy Association to PCF. <p>NOTE UE Policy Association is not supported in tests configured with Idle or Handover objectives.</p> <p>NOTE Establish UE Policy Association is supported only when Technical Spec Version is R16 or higher.</p>
Prefer AMF Change	Enable this option to change the AMF for an N2 handover even when the target RAN(T-RAN) is connected to the serving AMF.
<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.

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

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.

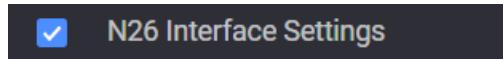
Connectivity Settings	Description
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix that has been assigned to this node.
Gateway Address	The IP address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

Connectivity Settings	Description
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.

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>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.

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.

AMF remote SBA nodes

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.

Setting	Description
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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer AUSF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
Peer AUSF	Select the peer AUSF using either of the following methods: <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. Refer to NF Discovery service for the steps required to use the discovery service.
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.
Indirect Communication without Delegated Discovery	IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings. Select the option to enable it. For more details, refer to Indirect Communication without Delegated Discovery .

Setting	Description
Indirect Communication with Delegated Discovery	<p>IMPORTANT This option is visible only when Peer AUSF is set to Discover and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to Indirect Communication with Delegated Discovery.</p>

UDM Connection Settings

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

Setting	Description
<i>UDM Connectivity Settings:</i>	
Use SBI Fuzzing	<p>Use the toggle button to enable this option.</p> <p>When enabled, the <i>Peer UDM</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.</p>
SBI Fuzzer	Select the node from the drop-down list.
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 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.
Indirect Communication without Delegated Discovery	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to Indirect Communication without Delegated Discovery.</p>
Indirect Communication with Delegated Discovery	<p>IMPORTANT This option is visible only when Peer UDM is set to Discover and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to Indirect Communication with Delegated Discovery.</p>

PCF Connection Settings

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

Setting	Description
<i>PCF Connectivity Settings:</i>	
Use SBI Fuzzing	<p>Use the toggle button to enable this option.</p> <p>When enabled, the <i>Peer PCF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.</p>
SBI Fuzzer	Select the node from the drop-down list.
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 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>	
Use SBI Fuzzing	<p>Use the toggle button to enable this option.</p> <p>When enabled, the <i>Peer SMF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.</p>
SBI Fuzzer	Select the node from the drop-down list.
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 for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nsmf communications. It can be either HTTP or

Setting	Description
	HTTPS.
Port	The SMF port number to use for Nsmf communications. The default is port 80, but you can choose a different port number.
Indirect Communication without Delegated Discovery	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to Indirect Communication without Delegated Discovery.</p>
Indirect Communication with Delegated Discovery	<p>IMPORTANT This option is visible only when Peer SMF is set to Discover and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to Indirect Communication with Delegated Discovery.</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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

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

- **Indirect Communication without Delegated Discovery** or
- **Indirect Communication with Delegated Discovery**

If Indirect Communication with or without Delegated Discovery option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which this option is enabled will be forwarded to the SCP. In the case of Indirect Communication with Delegated Discovery, SCP will also perform delegated discovery.

SEPP Connection Settings

To connect to the Security Edge Protection Proxy (SEPP) node, the following configuration settings are required.

Setting	Description
<i>SEPP Connection Settings:</i>	
Peer SEPP	Select either the IP address of a SCP node from your test network or <i>None</i> if you are not using one in your test configuration.
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.
Sepp Communication Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Telescopic FQDN • Target API Root

Home PLMN for Inter-PLMN Routing

The following configuration settings are required.

PLMN MCC	Provide the PLMN MCC value.
----------	-----------------------------

	<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>Provide the PLMN MNC value.</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>

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	211
AUSF Range panel	211
AUSF node settings	212
AUSF Nausf interface settings	213
AUSF Remote SBA Nodes	214

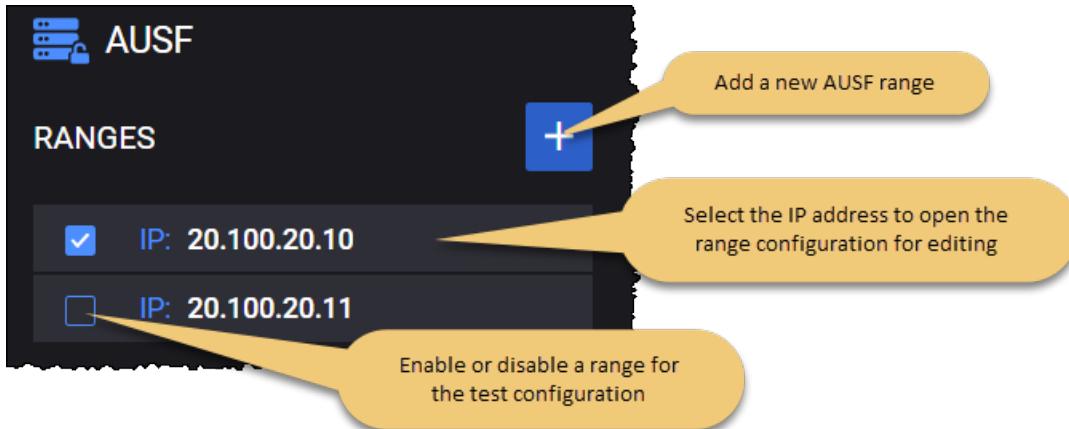
AUSF Ranges panel

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 it is selected in the Topology window).

Setting	Description
<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 .
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 .
Remote SBA Nodes	These settings are described in AUSF remote SBA nodes .

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 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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.

Connectivity Settings	Description
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer UDM</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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 for the steps required to use the discovery service.
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.
Indirect Communication without Delegated Discovery	<p>IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings. Select the option to enable it.</p>
Indirect Communication with Delegated Discovery	<p>IMPORTANT This option is visible only when Peer UDM is set to Discover and SCP is selected in SCP Connection Settings. Select the option to enable it.</p>

NOTE

If Indirect Communication with or without Delegated Discovery option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which this option is enabled will be forwarded to the SCP. In the case of Indirect Communication with Delegated Discovery, SCP will also perform delegated discovery.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

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.

LoadCore charging supports the collection and reporting of charging information for network resource usage using the CHF (Charging Function) node. The CHF enables charging services to be offered to authorized network functions (NFs).

LoadCore supports the Spending Limit Control Service functionality. The service enables the NF service consumer to retrieve policy counter status information—per UE—from the CHF by subscribing to spending limit reporting (that is, notifications of policy counter status changes). The following operations are supported by the service:

- **Subscribe:** This service operation is used by an NF service consumer to subscribe to notification of changes in the status of the policy counters available and retrieval of the status of the policy counters for which subscription is accepted.
- **Unsubscribe:** This service operation is used by an NF service consumer to send a request to the CHF to unsubscribe from notification of changes in the status of all policy counters.
- **Notify:** This service operation is used by the CHF in any of the following ways:
 - To notify the NF service consumers about the change of the status of the subscribed policy counters.
 - To provide one or more pending statuses for a subscribed policy counter, together with the time they shall be applied.
 - To send a notification to the NF service consumer requesting the termination of the subscription of status changes for all policy counters for a subscriber (for example: the subscriber is removed from the CHF system).

Converged Charging is a process where online and offline charging are combined. The charging information is utilized by CCS(Converged Charging System) in one converged charging service which offers charging with and without quota management, as well as charging information record generation.

Topics:

CHF Ranges panel	217
CHF Range settings	218
CHF node settings	219
CHF Nchf interface settings	219
CHF remote SBA nodes	220

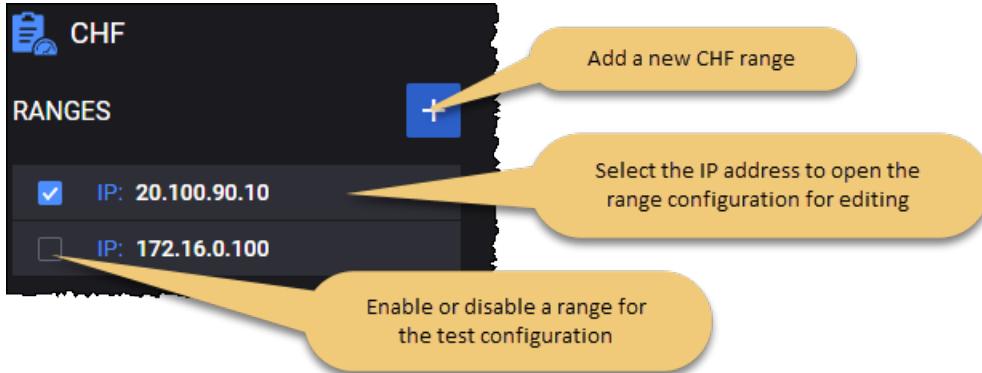
CHF Ranges panel

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 an CHF range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



CHF Range settings

You add and select CHF ranges from the CHF Ranges panel. When you select the IP address of CHF NRF range, 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 **Range Settings** that you configure 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 requires the configuration of an associated set of Node Settings, which are described in CHF node settings .

Setting	Description
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 .
Remote SBA Nodes	These settings are described in CHF remote SBA nodes .

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	Multiple CHF instances may be deployed in the 5G network. Each CHF 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.

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.

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 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.

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.
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.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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>	

Setting	Description
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.

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:

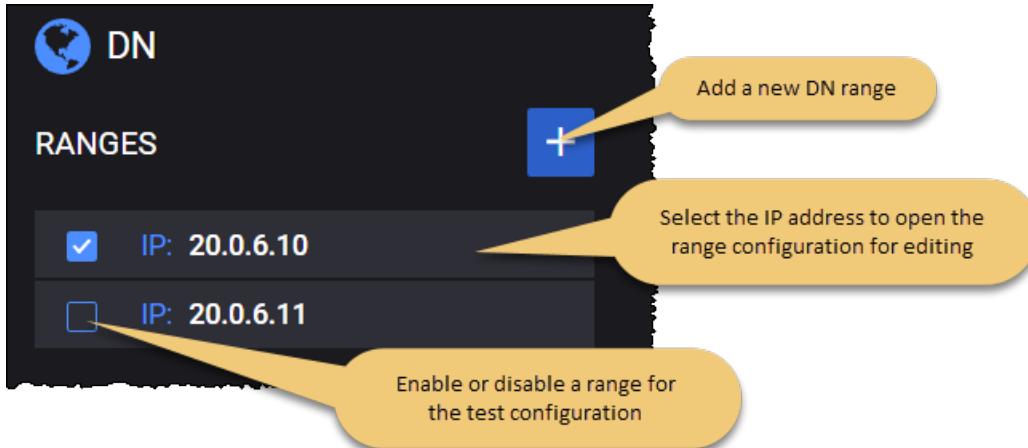
DN Ranges panel	223
DN Range panel	223
DN N6 interface settings	224
DN routes settings	225
DN User Plane	226
DN Stateless UDP Traffic	227
DN Data Traffic	228
DN Voice Traffic	231
DN Video OTT Traffic	241
DN DNS Server Traffic	244
DN Predefined Applications Traffic	246
DN Capture Replay	247

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 **Routes Settings** to configure the route to an UE or custom range.
- Select **User Plane** to configure the traffic generators.

DN range controls and settings

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

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

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

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

DN N6 interface settings

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

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

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 routes settings

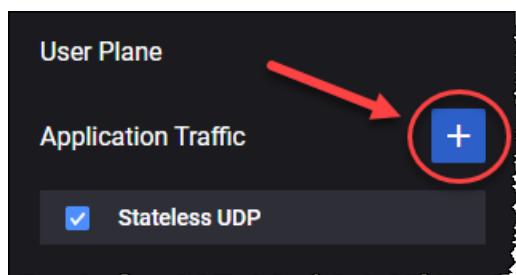
The following table describes the **Route Settings** that you need to configure in order to create the route to an UE or custom range.

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

Settings	Description
	<ul style="list-style-type: none"> specific DNNs: Select one or more of the individual DNNs from the list.
Destination Subnet Address	<p>Set the destination subnet address. This parameter is available only when the route type is set to Custom.</p>
IP Prefix Length	<p>The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address. This parameter is available only when the route type is set to Custom.</p>

DN User Plane

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



NOTE

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

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

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

DN Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Flow Type	This field is set to dowlink and can not be modified since on the DN you can only configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
Destination UE Range	Select the destination UE range from the drop-down list.

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

DN Data Traffic

The following table describes the DN Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Application Servers	<p>Each Application Traffic entry requires an application server definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"> To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings. To add another application server, click the Add Server button. LoadCore will open the Server panel where you will select the server type and configure the server settings. <p>Refer to Server (below) for a description of the configuration settings required by</p>

Parameter	Description
	<p>the application server.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

Server

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

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

Custom Parameters

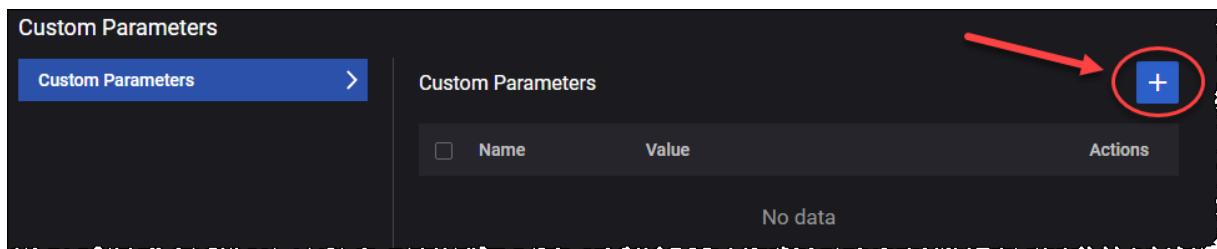
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

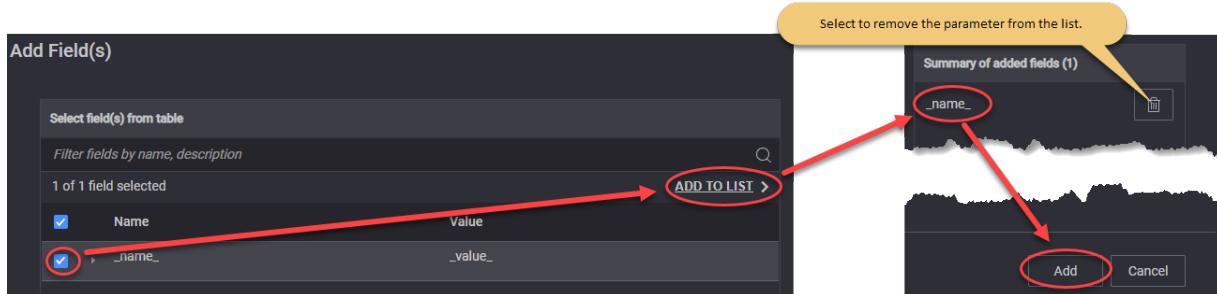
2. Select the **Add** button.



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 ...



DN Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Call Type	Select the type of call from the drop-down list.
Dial Plan:	<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

Parameter	Description
	overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security • UDP - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	For more details about these settings, refer to Media Settings .
<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.
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select the check box in order to enable this option.
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
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.

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.

Parameter	Description
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	Select the audio codec from the drop-down list. The available options are: <ul style="list-style-type: none"> • AMR - The Adaptive Multi-Rate (AMR) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • AMR-WB - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • EVS - The EVS (Enhanced Voice Services) codec specified by 3GPP TS 26.445 compresses 20ms input blocks of audio samples. In addition to the EVS Primary mode, 3GPP TS 26.445 specifies that the codec implement the EVS AMR-WB IO mode for interoperability with AMR WB devices. • PCMU • PCMA • iLBC • G722 • G723 • G729 The parameters of each audio codec are presented below.
<i>Advanced Media Settings</i>	
Custom SDP	Select this panel to open the custom SDP settings.
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4

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

AMR/AMR-WB

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

EVS

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

Parameter	Description
	<ul style="list-style-type: none"> 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.

Advanced SIP Settings

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

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

SIP Custom Headers

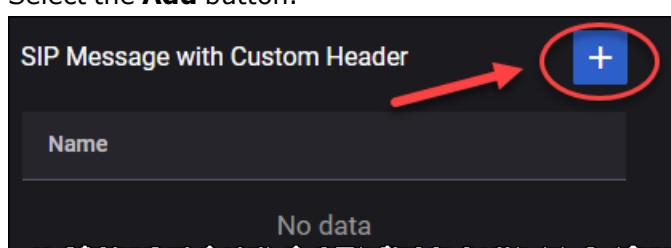
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE

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

For each message, you can:

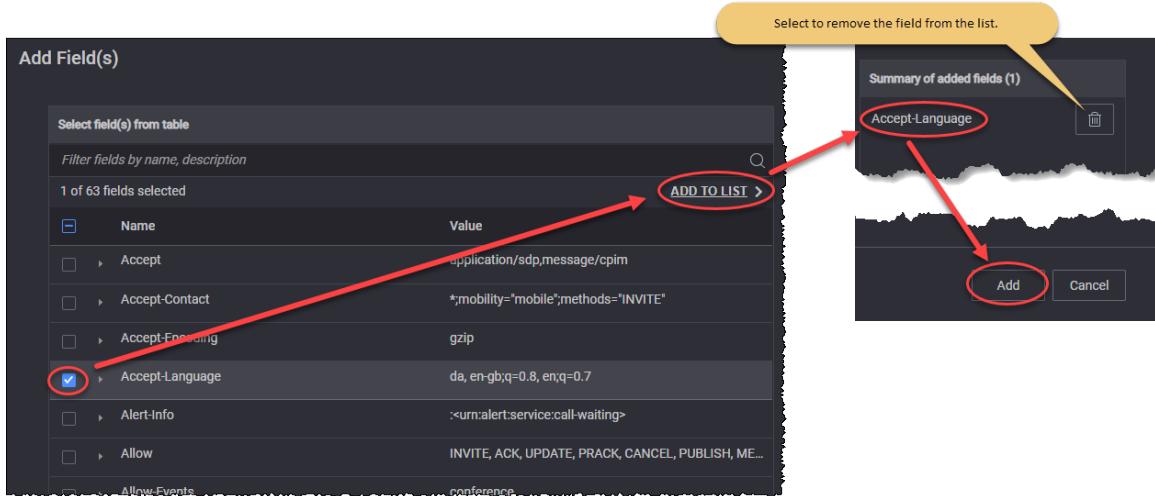
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
 - Select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom header are available:

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

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

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

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

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

SIP Authentication

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

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

Parameter	Description
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by 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.

DN Video OTT Traffic

The following table describes the Video OTT Traffic parameters.

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

Parameter	Description
	Select this button to add an OTT server to your test configuration.
	Select this button to remove the OTT server from the test configuration.
Server Name	Set the server name. Each server is identified by a unique name. You can accept the value provided by 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 • HTTP/QUIC
Port	Set the port number. 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.
Streams	Refer to Streams (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Streams

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



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

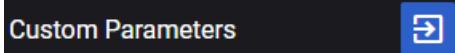
Parameter	Description
	Select this button to add a stream to your test configuration.
	Select this button to remove the stream from the test configuration.
Stream Name	Set the stream name. Each server is identified by a unique name. You can accept the value provided by LoadCore or overwrite it with your 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

Parameter	Description
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.
<i>Quality Levels:</i>	<i>Set the quality value for each level.</i>
	Select this button to add a quality level to your test configuration.
	Select this button to remove the quality level from the test configuration.
Bitrate (kbps)	Set the value of the bitrate.
Resolution	Select the resolution from the drop-down list. Available options: QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K .
Frames per second	Set the number of frames per second.

Custom Parameters

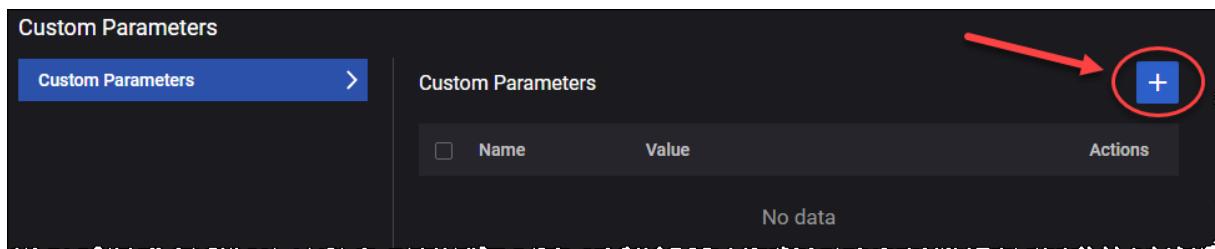
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

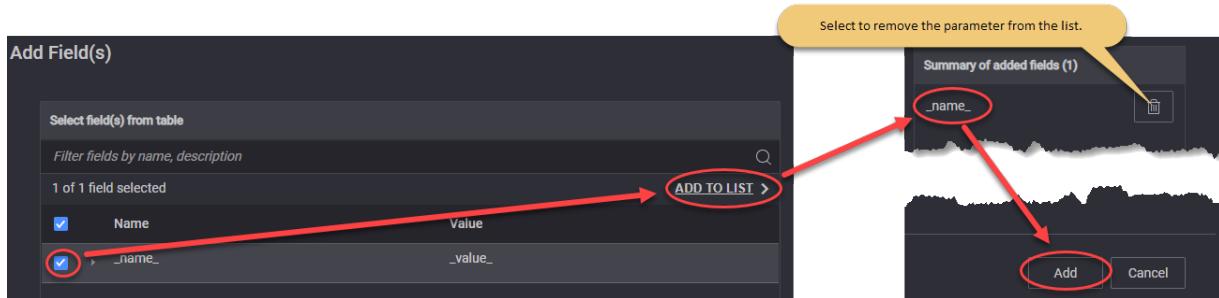
2. Select the **Add** button.



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 ...



DN DNS Server Traffic

The following table describes the DNS Server Traffic parameters.

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

Parameter	Description
	Select this button to remove the DNS server from the test configuration.
Type	Select the type from the available options.
Port	Set the port number. You can accept the 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.
Zone Manager	Refer to Zone Manager (below) for descriptions of the DNS server zones settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Zone Manager

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



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

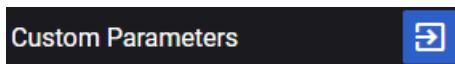
Parameter	Description
	Select this button to add a zone to your test configuration.
	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by LoadCore or overwrite it with your own value.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

Parameter	Description
	<ul style="list-style-type: none"> • CNAME • TXT • PTR • NS
Hostname	Set the hostname.
Address	Provide the address.

Custom Parameters

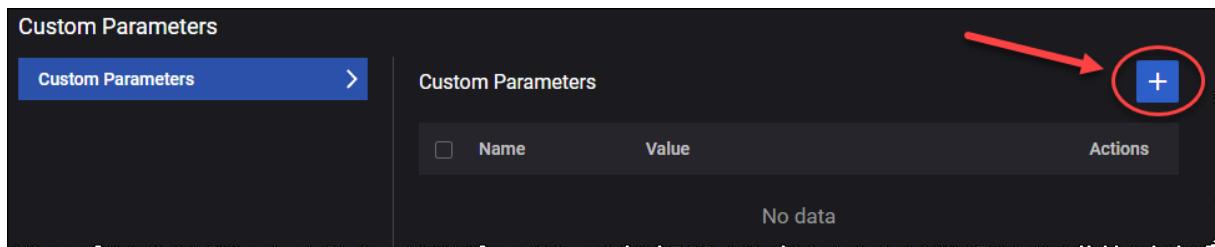
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

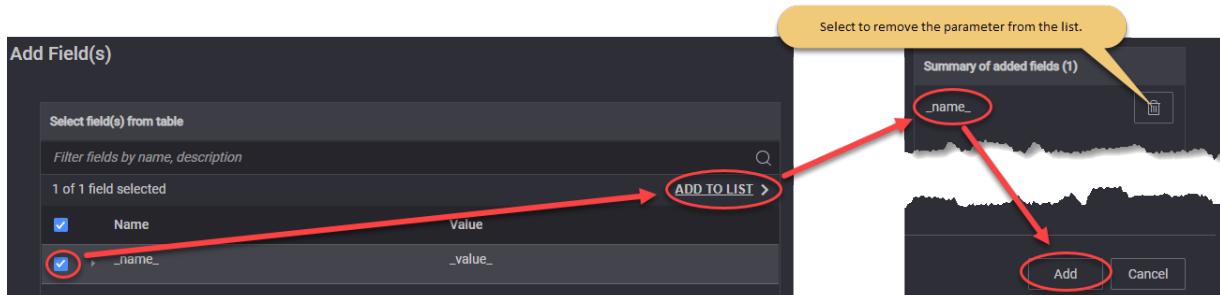
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DN Predefined Applications Traffic

The following table describes the Predefined Applications parameters.

Parameter	Description
Application	Select the type of traffic you want to generate. In this case, this parameter must

Parameter	Description
Type	be set to Predefined Applications .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Predefined Traffic Profiles	Select the traffic profile from the available options.

DN Capture Replay

The following table describes the Capture Replay parameters.

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

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

The following table describes the Filter object parameters.

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

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

DNS Server configuration settings



LoadCore includes simulation and isolation for DNS Server node.

The configuration settings are described in the topics listed below.

Topics:

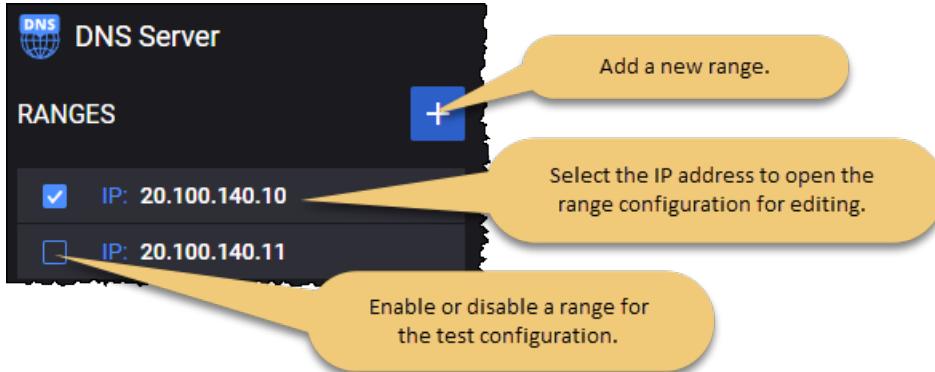
DNS Server Ranges panel	250
DNS Server Range panel	250
DNS Server Ndnsserver interface settings	251
DNS Server Traffic Flow settings	252

DNS Server Ranges panel

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

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

For example ...



DNS Server Range panel

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

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

DNS Server range controls and settings

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

The following table describes the available **Range** configuration options for each DNS Server 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 DNS Server is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the DNS Server functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Ndnsserver Interface Settings	Each DNS Server range requires the configuration of an interface necessary for connectivity. These settings are described in DNS Server Ndnsserver interface settings .
Traffic Flow Settings	These settings are described in DNS Server Traffic Flow settings .

DNS Server Ndnsserver interface settings

The following **Connectivity Settings** enable the necessary DNS Server connectivity.

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

Connectivity Settings	Description
MAC	<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.

DNS Server Traffic Flow settings

The following table describes the DNS Server Traffic Flow parameters.

Parameter	Description
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Zone Manager	Refer to Zone Manager (below) for descriptions of the DNS server zones settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Zone Manager

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



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

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

Custom Parameters

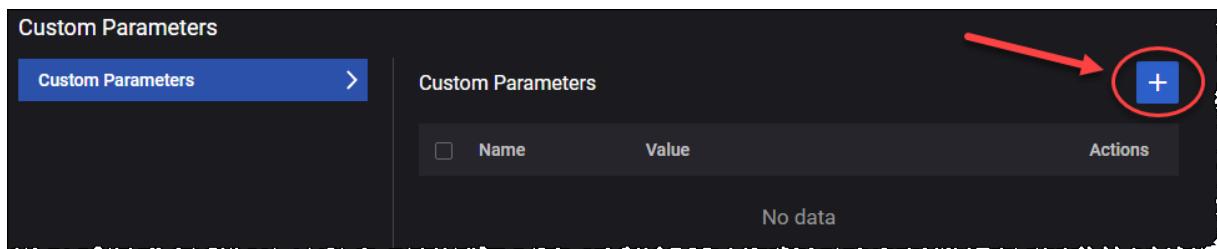
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...

Add Field(s)

Select field(s) from table

Filter fields by name, description

1 of 1 field selected

Name	Value
<input checked="" type="checkbox"/> _name_	_value_

ADD TO LIST >

Summary of added fields (1)

name

Add Cancel

Select to remove the parameter from the list.

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	255
CSCF N6 interface settings	256
CSCF Rx interface settings	257
CSCF UE routes settings	258
Media Function Range panel	259

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).
<i>Range Settings:</i>	
P-CSCF Node Settings	
Domain	Set the domain name.

Setting	Description
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Authentication Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: keysight.com .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: Digest , AKAv2 or AKAv1 .
Algorithm	Select the algorithm from the drop-down list. Available options: MD5 , MD5-Sess , SHA256 or SHA256-Sess .
Quality of Protection	Select an option from the drop-down list: auth or auth-init .
<i>AF Node Settings</i>	
Hostname	Set the hostname.
Realm	Set the realm. Default value: keysight.com .
<i>N6 Interface Settings</i>	<i>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.</i>
<i>Rx Interface Settings</i>	<i>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.</i>
<i>UE Routes Settings</i>	<i>These settings are described in CSCF UE routes settings.</i>
<i>Remote SBA Nodes</i>	
Peer PCRF	Select the IP address of the PCRF node.

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
<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>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.
<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.

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
<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.

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.

Settings	Description
<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.

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>	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 Settings	Description
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 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	262
MME Range panel	263
MME node settings	264
MME S11 Interface Settings	265
MME N26 Interface Settings	266
MME S1 Interface Settings	267
MME S6a Interface Settings	269
MME Diameter settings	270

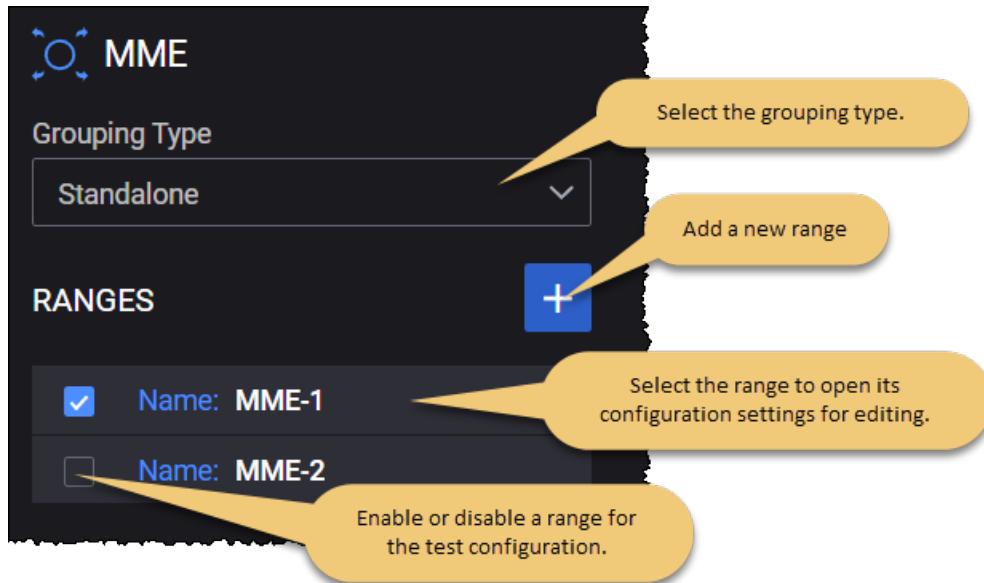
MME Ranges panel

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.
- Add a new MME range to your test configuration.
- 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
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 .
IMPORTANT	All the interfaces are enabled automatically if the MME Grouping Type is set to Standalone and the S1 interface IP configuration becomes mandatory.

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 .
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 .
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 .
S1 Interface Settings	These settings are described in MME S1 Interface settings .
S6a Interface Settings	These settings are described in MME S6a Interface settings .

Setting	Description
Diameter Settings	These settings are described in MME Diameter settings .

MME node settings

Each MME range includes a set of Node Settings.

Node Settings

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

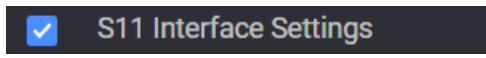
Setting	Description
Name	A name uniquely identifies each MME range. You can accept the value provided by LoadCore or overwrite it with your own value.
Group ID	The MME Group Identifier to which this MME is assigned. The MME Group Identifier is a 16-bit value that is unique within a PLMN. The valid range 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
Relative Capacity	Set the relative capacity value.

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.

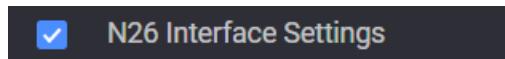
Connectivity setting	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the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

Connectivity setting	Description
Increment	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 <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

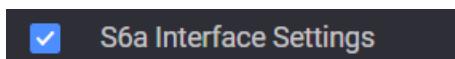
Connectivity setting	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits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

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.

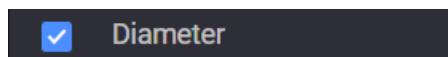
NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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	<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 Diameter settings

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.

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:

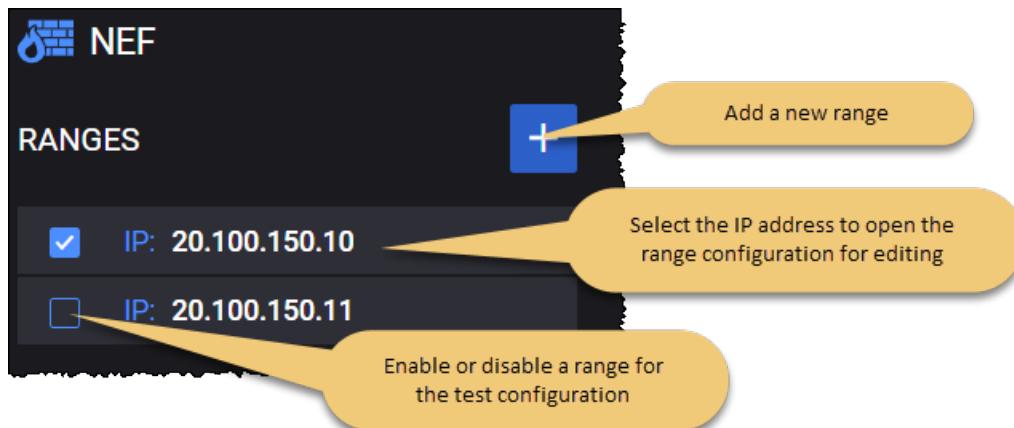
NEF Ranges panel	271
NEF Range panel	271
NEF Nnrf interface settings	272
NEF Remote SBA Nodes	273

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	Each AMF range requires the configuration of an associated set of Node Settings, which are described in NEF node settings .
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 .
Remote SBA Nodes	The remote SBA node settings are described in NEF Remote SBA Nodes .

NEF 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
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.

Connectivity Settings	Description
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer PCF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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 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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer UDM</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.
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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer UDR</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

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	277
NRF Range panel	277
NRF node settings	278
NRF Nnrf interface settings	279
NRF Remote SBA Nodes	280

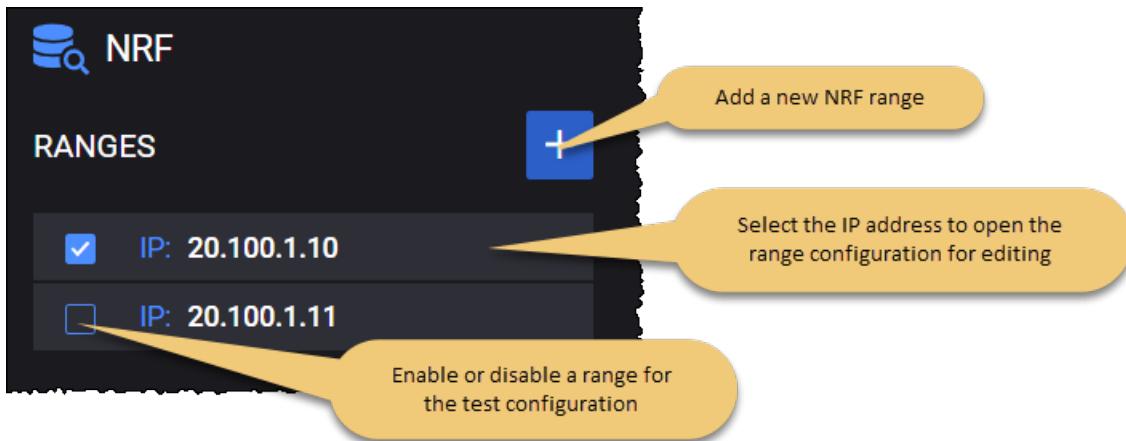
NRF Ranges panel

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 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

Setting	Description
	is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each NRF range requires the configuration of an associated set of Node Settings, which are described in NRF node settings .
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 .

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
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).
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

NRF Remote SBA Nodes

Remote SEPP

To connect to the peer Security Edge Protection Proxy (SEPP) node, the following configuration settings are required.

Setting	Description
Peer SEPP	Select either the IP address of a SCP node from your test network or <i>None</i> if you are not using one in your test configuration.
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.
Sepp Communication Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Telescopic FQDN • Target API Root
Force FQDN Mapping	Select this option to enable it.

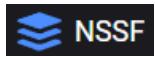
Remote NRFs

The following configuration settings are required.

Setting	Description
<i>Remote NRFs :</i>	
	Select the Add Remote NRF button to add a new remote NRF to your test configuration.
<i>Remote NRF:</i>	
	Select the Delete Remote NRF button to delete the remote NRF range from your test configuration.
Peer NRF	Select the IP address of the peer NRF.

Setting	Description
FQDN	<p>The value has the following form: <code><instanceID>.5gc.mnc<value1>.mcc<value2>.3gppnetwork.org:</code></p> <ul style="list-style-type: none"> • <code>instanceID</code> of the selected remote NRF • <code>value1</code> is the PLMN MNC of the selected remote NRF and should always have 3 digits, padded with zeros (04 should be 004) • <code>value2</code> is the PLMN MCC of the selected remote NRF
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	283
NSSF Range panel	283
NSSF node settings	284
Nnssf Interface Settings	285
Remote SBA nodes	286
NSSF Restricted NSSAIs	287
NSSF Network Slices	288
NSSF Configured NSSAI	289

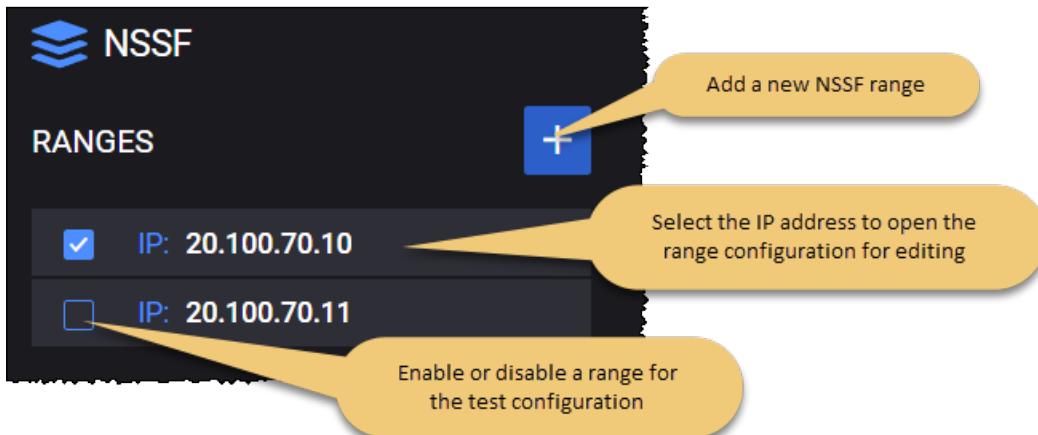
NSSF Ranges panel

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.
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.

Setting	Description
	(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 .
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 .
Remote SBA Nodes	These settings are described in Remote SBA nodes .
<i>Network Slicing:</i>	
Restricted NSSAIs	These settings are described in NSSF Restricted NSSAIs .
Network Slices	These settings are described in NSSF Network Slices .
Configured NSSAIs	These settings are described in NSSF Configured NSSAI .

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	<p>Multiple NSSF instances may be deployed in the 5G network.</p> <p>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.</p>
PLMN 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>

Setting	Description
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

Connectivity Setting	Description
<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>	
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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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 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.

Setting	Description
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>	

Setting	Description
	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



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/PCRF Ranges panel	291
PCF Range panel	292
PCF node settings	293
PCRF node settings	294
PCF service area restrictions	294
PCF Npcf interface settings	296
PCRF Rx interface settings	297
PCF remote SBA nodes	298

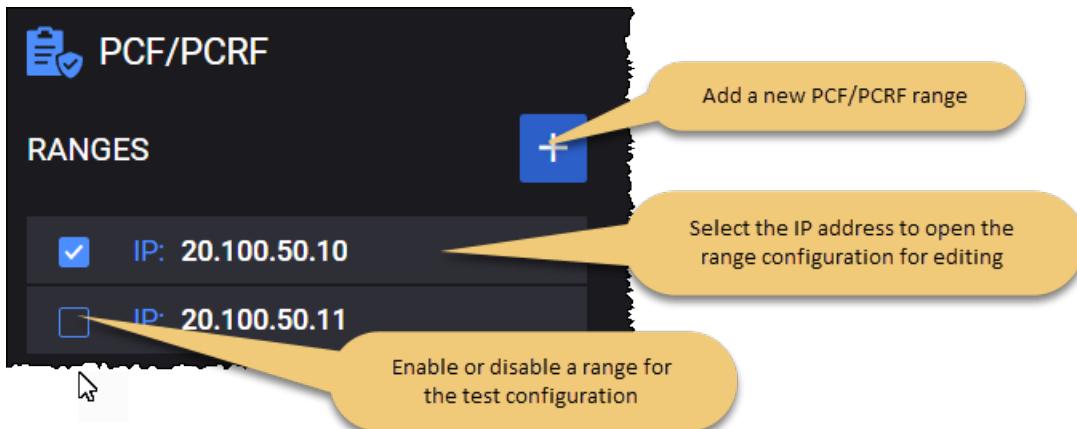
PCF/PCRF Ranges panel

The **PCF/PCRF Ranges** panel opens when you select the PCF/PCRF 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 ...



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 described in PCF node settings .
PCRF Node Settings	These settings are described in 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 .
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 .
Rx Interface Settings	The Rx interface settings are available only when PCRF Node Settings option is selected. These settings are described in Rx Interface Settings .
Remote SBA Nodes	These settings are described in PCF remote SBA nodes .

PCF node settings

Each PCF range includes a set of Node Settings.

Node Settings

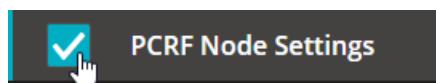
Each PCF instance (that is, each range) is identified by the following node settings.

Setting	Description
Instance ID	Multiple PCF instances may be deployed in the 5G network. 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.
PLMN MCC	The PLMN MCC for this PCF 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 PCF 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.
RFSP	The value of RAT/Frequency Selection Priority (RFSP) index.
Triggers	Request Triggers to which the PCF subscribes. The allowed values are: <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. Both values can be selected simultaneously.
Include Request in Response	Enable this option to include the request in the response message.
Default Charging Method Offline	If needed, enable this option.

Setting	Description
Default Charging Method Online	If needed, enable this option.
Ask RResult Notification from SMF for Create/Delete QoS Flow	If needed, enable this option.
RAT Type Awareness	Select an option from the drop-down list: <ul style="list-style-type: none"> • Ignore • 5G Only • 4G Only

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:

Setting	Description
	<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.
<i>Area:</i>	
	Select the Delete Area button to remove the restriction area from your configuration.
Area Codes	<p>Set the area code. 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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.

Connectivity Settings	Description
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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
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).
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.

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

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>	
Use SBI Fuzzing	<p>Use the toggle button to enable this option.</p> <p>When enabled, the <i>Peer UDR</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.</p>
SBI Fuzzer	Select the node from the drop-down list.
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 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>	
Use SBI	Use the toggle button to enable this option.

Setting	Description
Fuzzing	When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

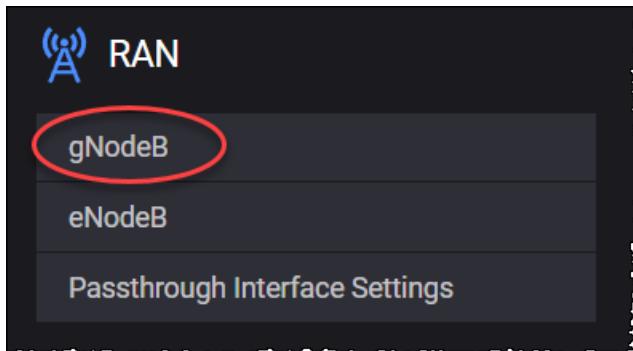
The configuration settings are described in the topics listed below.

Topics:

gNodeB	301
gNodeB Ranges panel	302
gNodeB Range settings	307
gNodeB node settings	308
gNodeB NSSAI settings	310
gNodeB N2 interface settings	311
gNodeB N3 interface settings	313
eNodeB	316
eNodeB Ranges panel	317
eNodeB Range Settings	321
eNodeB Node Settings	321
Passthrough interface settings	323

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	302
gNodeB Range settings	307
gNodeB node settings	308
gNodeB NSSAI settings	310
gNodeB N2 interface settings	311
gNodeB N3 interface settings	313

gNodeB Ranges panel

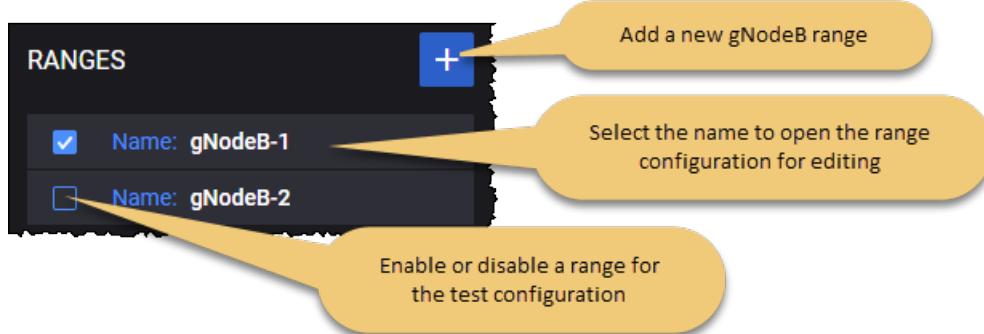
The **gNodeB Ranges** panel opens when you select **gNodeB** from the RAN pane. It consists of two main section: Ranges and Ranges Connectivity.

Ranges

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

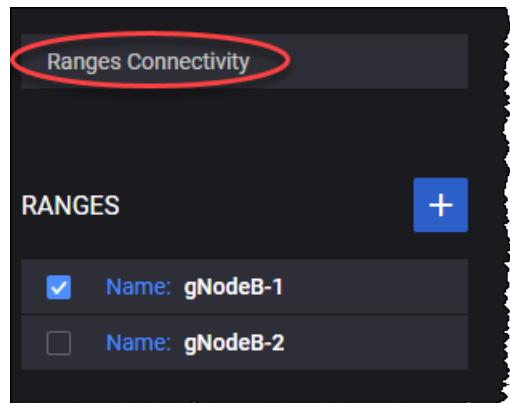
- Add a new gNodeB range to your test configuration.
- Open a gNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



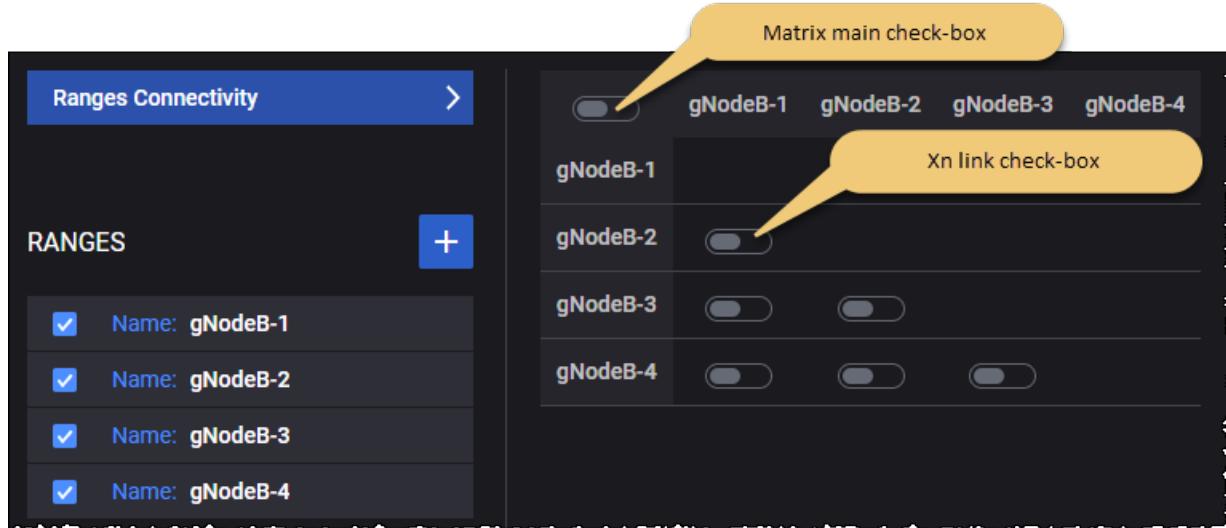
Ranges Connectivity

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.



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

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

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

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

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

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

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

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.

	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6
gNodeB-1	<input type="checkbox"/>					
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"/>
gNodeB-6					<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 screenshot shows the 'Ranges Connectivity' interface. On the left, there's a list of 'RANGES' with checkboxes next to each name. The names listed are: gNodeB-1, gNodeB-2, gNodeB-3, gNodeB-4, gNodeB-5, gNodeB-6, and gNodeB-7. The checkboxes for gNodeB-1, gNodeB-2, gNodeB-5, gNodeB-6, and gNodeB-7 are checked. To the right of this list is a 7x7 matrix of checkboxes. The columns and rows are labeled gNodeB-1 through gNodeB-7. The first column contains a main checkbox at the top, which is checked. Below it, the checkboxes for gNodeB-1 are checked. The other columns (gNodeB-2 to gNodeB-7) have their first row's checkbox checked, while the rest are unselected.

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

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

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

This screenshot is similar to the one above, but the main matrix check-box at the top-left of the 7x7 grid is now circled in red and checked. All the other checkboxes in the matrix are also checked, indicating that selecting the main matrix check-box results in all Xn links being selected.

Even the Xn link check-boxes for disabled gNodeB ranges are selected since the Xn links for disabled gNodeB ranges are not sent to the traffic agent. This way, when the disabled gNodeB range is

enabled, you will not have to manually select the Xn link check-boxes for that particular gNodeB range.

gNodeB Range settings

You add and select gNodeB ranges from the gNodeB Ranges panel. When you select the name of an gNodeB range, 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 .
NSSAI	Each gNodeB range requires the configuration of at least one NSSAI, and may specify multiple NSSAIs. These settings are described in gNodeB NSSAI settings .
N2 Interface Settings	Each gNodeB range requires the configuration of N2 interface settings, through which a gNodeB instance enables connectivity and interaction with the AMF component in the 5G network. These settings are described in gNodeB N2 interface settings .
N3 Interface Settings	Each gNodeB range requires the configuration of N3 interface settings, through which a gNodeB instance enables connectivity and interaction with the UPF component in the 5G network. These settings are described in gNodeB N3 interface settings .

gNodeB node settings

Each gNodeB range includes a set of Node Settings.

Node Settings

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

Setting	Description
Name	Multiple gNodeB instances may be deployed in the 5G network. Each gNodeB instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by 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.
gNodeB ID Length	The number of bits from the Cell Identity to use as the gNodeB ID.
Cell ID	The NR Cell Identity (NCI) for the cell associated with this node range.
Connection Timeout (ms)	The S1AP connection timeout.
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.

EPS Fallback Settings

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

The following parameters are required to configure the EPS fallback:

Setting	Description
Enable EPS	Select the check box to enable this option.

Setting	Description
Fallback	
5QI	<p>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 101 panel in the Global Settings.)</p> <p>When a request is received for this 5QI to create a dedicated QoS flow, the RAN will reject the request, which will trigger the EPS fallback procedure.</p>
Associated ENB	Select the eNodeB used for handover.
Secondary Node	<p>Select the secondary node from the drop-down list.</p> <p>This option is used for EPS fallback to an eNodeB associated to a gNodeB using Option 3x.</p>
EPS Fallback Mobility	<p>Type of mobility to EPS during EPS fallback.</p> <p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • Handover to 4G • Inter-System Redirection to 4G
EPS Fallback Return Mobility	<p>Type of mobility that occurs after the deletion of the dedicated bearer that triggered EPS fallback.</p> <p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • None - After the dedicated bearer is deleted in 4G, the UE will not initiate any procedure. • Connected Mode Handover to 5G (default value) - After the dedicated bearer is deleted in 4G, the UE will initiate a 4G to 5G Connected Mode Handover. • Idle Mode Mobility to 5G - After the dedicated bearer is deleted in 4G, the UE will perform an Enter Idle procedure in 4G, followed by a 4G to 5G iRAT Idle Mode Mobility.

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

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

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

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

Setting	Description
Public Warning System	Select the check box to enable this option.

Setting	Description
PWS Restart Timer (s)	Duration in seconds after which PWS Restart Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.3 PWS Restart Indication</i> .
PWS Failure Timer (s)	Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.4 PWS Failure Indication</i> .

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, NASSAI 2,...NASSAI X) as required to meet your test objectives.

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

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

Setting	Description
NSSAI:	
	Select the Add NSSAI button to add a new NSSAI to your test configuration.
NSSAI settings:	
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.
SST	The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:

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

gNodeB N2 interface settings

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

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

By default, the N2 interface check box is enabled.

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

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

N2 Interface Settings

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

Settings	Description
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum Retransmission Timeout (ms)	Set the maximum retransmission timeout value, in milliseconds.
Initial Retransmission Timeout (ms)	Set the initial retransmission timeout value, in milliseconds.
Maximum Retransmission per Association	Set the maximum retransmissions value per association.
Maximum Retransmission per Path	Set the maximum retransmissions value per path.
Heartbeat Interval (ms)	Set the heartbeat interval value, in milliseconds.
SACK Delay (ms)	Set the delayed selective ACK timeout value.
SACK Frequency	Set the delayed selective ACK frequency value.

Connectivity Settings

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).

Settings	Description
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>
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..

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.

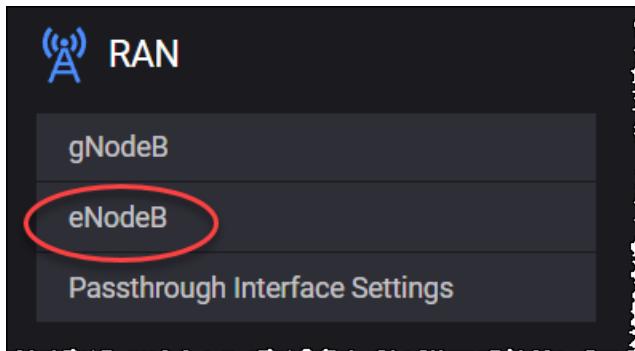
NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<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.
<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	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.

Connectivity Settings	Description
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:

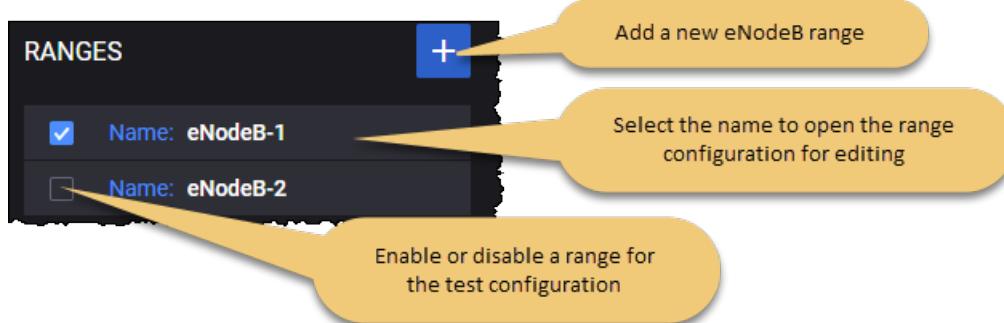
eNodeB Ranges panel	317
eNodeB Range Settings	321
eNodeB Node Settings	321

eNodeB Ranges panel

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

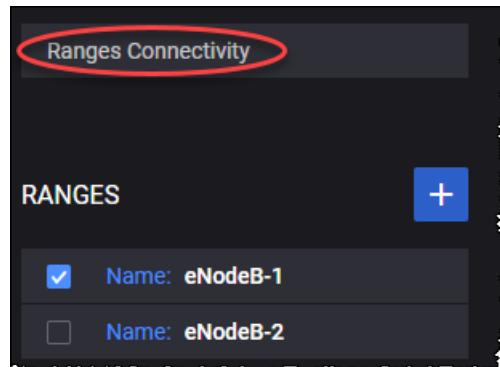
- Add a new eNodeB range to your test configuration.
- Open a eNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



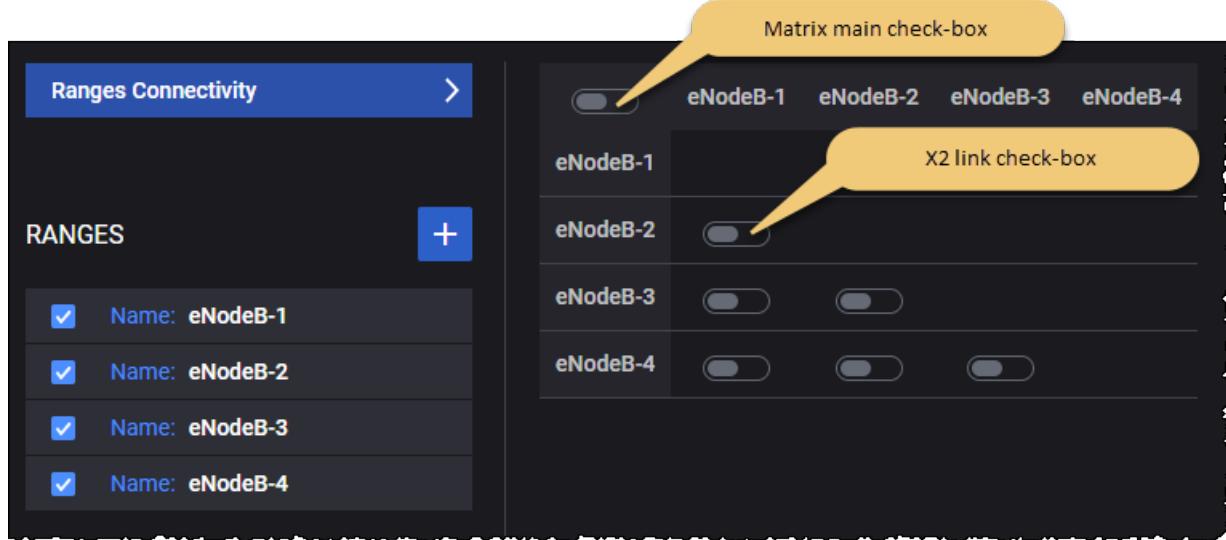
Ranges Connectivity

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



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

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



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

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

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

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

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

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

The screenshot shows the 'Ranges Connectivity' interface. On the left, under 'RANGES', the range 'eNodeB-4' has a greyed-out checkbox. In the main area, the 'eNodeB-4' row and column in the connectivity matrix are also greyed out, indicating they are disabled.

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

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

For example ...

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

The screenshot shows the 'Ranges Connectivity' interface. The range 'eNodeB-4' is highlighted with a red oval in the RANGES list, and its switch in the matrix is also highlighted with a red oval. The range 'eNodeB-3' is also highlighted with a red oval in the RANGES list, and its switch in the matrix is checked and highlighted with a red oval.

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

The screenshot shows the 'Ranges Connectivity' interface. On the left, there's a sidebar titled 'RANGES' with a '+' button. Below it is a list of eNodeB ranges with checkboxes next to their names: eNodeB-1 (checked), eNodeB-2 (checked), eNodeB-3 (unchecked), eNodeB-4 (unchecked), eNodeB-5 (checked), eNodeB-6 (checked), and eNodeB-7 (checked). To the right is a matrix of checkboxes for X2 links between eNodeBs. The columns are labeled eNodeB-1 through eNodeB-7. The first column (eNodeB-1) has a main checkbox at the top. The matrix cells contain smaller checkboxes. For example, the cell at row eNodeB-2, column eNodeB-3 contains a checked box. The entire matrix is surrounded by a dashed border.

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

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

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

This screenshot is similar to the one above, but the main matrix check-box at the top of the first column is now checked and highlighted with a red circle. All other X2 link checkboxes in the matrix are also checked, indicating they are all selected.

Even the X2 link check-boxes for disabled eNodeB ranges are selected since the X2 links for disabled eNodeB ranges are not sent to the traffic agent. This way, when the disabled eNodeB range is

enabled, you will not have to manually select the X2 link check-boxes for that particular eNodeB range.

eNodeB Range Settings

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

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

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

eNodeB Node Settings

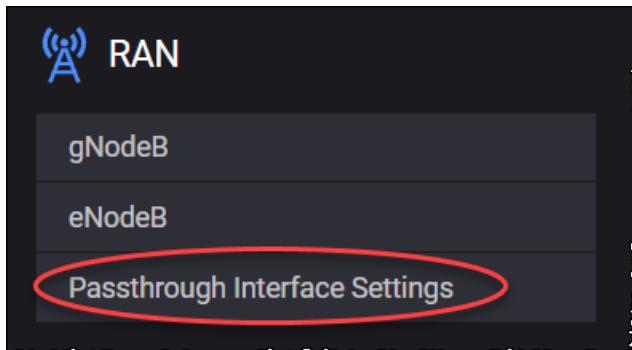
Each eNodeB instance (that is, each range) is identified by the following node settings.

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.
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

Setting	Description
	identifies a cell within the eNodeB. The same Cell Identifier is used for each eNodeB defined in a range.
Connection Timeout (ms)	The S1AP connection timeout.
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.

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.

SBI Fuzzer configuration settings



SBI Fuzzer intercepts requests and responses from a node and applies different modification algorithms to the message's body. SBI Fuzzer only modifies messages that contain a JSON body (content-type: application/json).

The configuration settings are described in the topics listed below.

Topics:

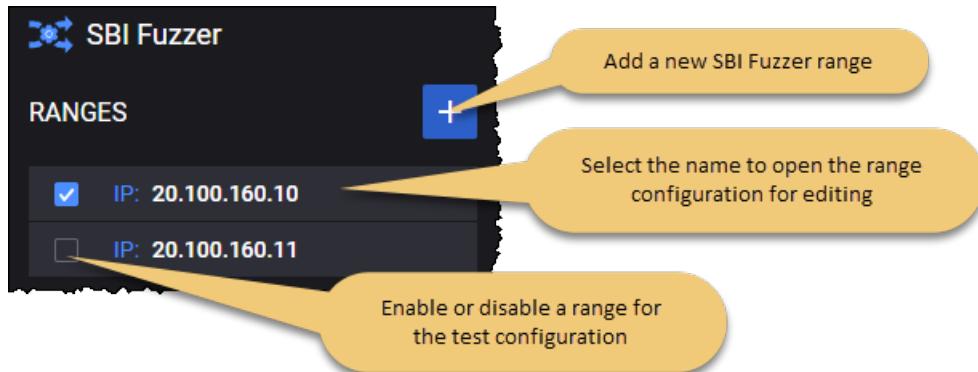
SBI Fuzzer Ranges panel	325
SBI Fuzzer Range panel	325
SBI Fuzzer interface settings	327
SBI Fuzzer Target Node	328

SBI Fuzzer Ranges panel

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

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

For example ...



SBI Fuzzer Range panel

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

- Select the **Delete Range** button to delete the selected SBI Fuzzer range from the test configuration.
- Use the **Range Settings** to configure the node and connectivity settings for the SBI Fuzzer range.

SBI Fuzzer range controls and settings

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

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

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

SBI Fuzzer Node Settings

The following table describes the available SBI Fuzzer Node Settings.

Setting	Description
Instance ID	Each SBI Fuzzer 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.
Fuzzed Messages	Select from the drop-down the type of HTTP message the fuzzing algorithm should be applied to. Available options: <ul style="list-style-type: none"> • Requests Only • Responses Only • Requests and Responses
Fuzzing Algorithm	Select the fuzzing algorithm type from the drop-down list. Available options: <ul style="list-style-type: none"> • Forward Unchanged - does not modify the original body. • Duplicated JSON Values - duplicates a random key-value pair from the original body. • Extra JSON Values - adds extra key-value pairs that are generated randomly to the original body. • Extra Spaces - adds extra spaces. • Integer Overflow - modifies integer value to an overflow value. • Duplicated JSON Entries With Wrong Values - duplicates a random key

Setting	Description
	from the original body and modifies its value to a random string.
NOTE	Although <code>content-type: multipart/related</code> may contain JSON parts, this type of message will not be fuzzed.
NOTE	SBI Fuzzer cannot be used in combination with SCP or SEPP.
NOTE	Messages with <code>content-type: application/problem+json</code> will not be modified.
NOTE	Impairment script cannot be applied to the agent on which SBI Fuzzer runs on.

SBI Fuzzer interface settings

The following **Connectivity Settings** enable the necessary SBI Fuzzer connectivity.

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.
Additional Routes	<i>The additional route is needed if the source IP is not of a node simulated in LoadCore.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost

Connectivity Settings	Description
	bits in the address, which indicates the network portion of the address.
<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.

SBI Fuzzer Target Node

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

Setting	Description
SBA Peer	Select the peer node from the drop-down list. Available options: None (default value), NRF , AUSF , PCF , UDR , NSSF , SMSF , EIR , CHF , SEPP , AMF , UDM , NEF , SMF , SCP .
IP Address	Set the IP address of the peer node.
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.

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:

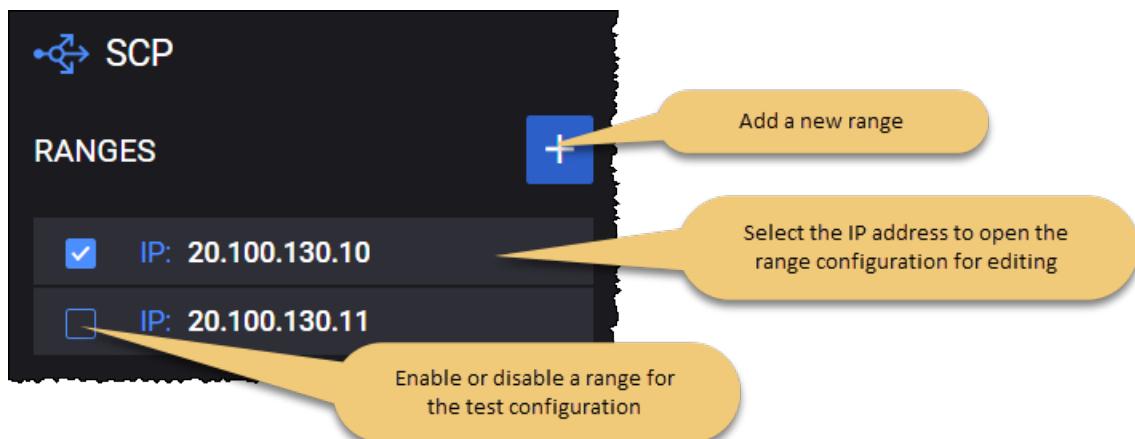
SCP Ranges panel	329
SCP Range panel	329
SCP interface settings	331
SCP Remote SBA Nodes	332

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	Each SCP range requires the configuration of an associated set of Node Settings, which are described in SCP Node Settings .
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 .
Remote SBA Nodes	The remote SBA node settings are described in SCP Remote SBA Nodes .

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 option to enable SCP Chaining. The SCP will be able to forward the messages it receives to a different SCP.
Enable Delegated Discovery	Select this option to enable delegated discovery.
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
<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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<i>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.
<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.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

SEPP configuration settings



The Security Edge Protection Proxy (SEPP) enables secure interconnect between 5G networks. The SEPP ensures end-to-end confidentiality and/or integrity between source and destination network for all 5G interconnect roaming messages.

The Security Edge Protection Proxy (SEPP) is a non-transparent proxy and supports the following functionality:

- Message filtering and policing on inter-PLMN control plane interfaces.

NOTE

The SEPP protects the connection between Service Consumers and Service Producers from a security perspective, i.e. the SEPP does not duplicate the Service Authorization applied by the Service Producers as specified in clause 7.1.4 (TS 23 501).

- Topology hiding.

Detailed functionality of SEPP, related flows and the N32 reference point, are specified in TS 33.501.

The configuration settings are described in the topics listed below.

Topics:

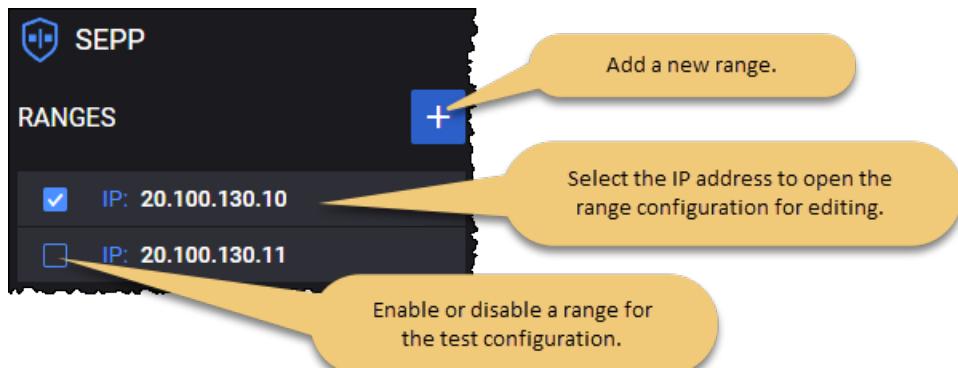
SEPP Ranges panel	333
SEPP Range panel	334
SEPP Nsepp interface settings	335
SEPP Remote SBA Nodes	336

SEPP Ranges panel

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

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

For example ...



SEPP Range panel

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

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

SEPP range controls and settings

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

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

SEPP Node Settings

The following table describes the available SEPP Node Settings.

Setting	Description
Instance ID	Each SEPP 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 range. About PLMN MCC ... A Public Land Mobile Network (PLMN) is a telecommunications network that

Setting	Description
	<p>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 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>
HTTP Connections	The number of HTTP connections between two nodes.
Use 3gpp-sbi-target-apiroot	Select this option to enable it.
Handle HTTP As HTTPS	Select this option to enable it. This is used to debug the HTTPS messages that are forwarded by SEPPs.

SEPP Nsepp interface settings

The following **Connectivity Settings** enable the necessary SEPP connectivity.

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.

Connectivity Settings	Description
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

SEPP 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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

Peer SEPP Nodes

Setting	Description
<i>Peer SEPP Nodes:</i>	
	Select the Add Peer SEPP button to add a new peer SEPP to your test configuration.
<i>Peer SEPP:</i>	
	Select the Delete Peer SEPP button to delete the peerSEPP range from your test configuration.
Peer SEPP	Select the IP address of the peer SEPP.
Initiate Handshake	Select this option to enable it.

DNS Server Connection Settings

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

Setting	Description
Peer DNS	Select the IP address of the peer DNS server.
Protocol	The protocol to use for communications. It can be either TCP or UDP.
Port	The port number to use for communications.

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	339
SGW Range panel	340
SGW S1-U Interface Settings	341
SGW S5-C Interface Settings	342
SGW S5-U Interface Settings	343
SGW S11 Interface Settings	344
SGW DUT S11 Interface Settings	345

SGW Ranges panel

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

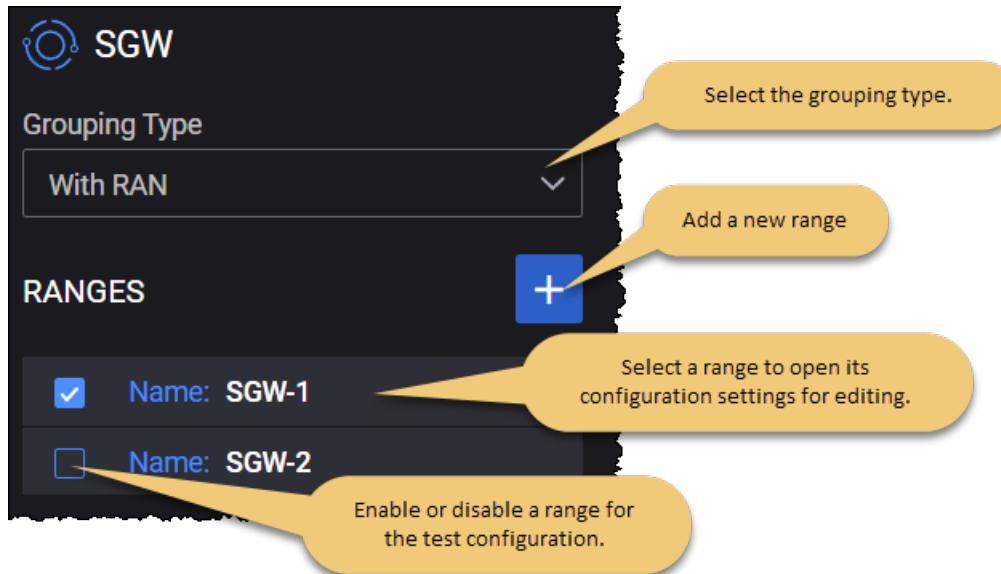
The following configuration option is available on this panel:

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 .
S5-c	Each SGW range requires the configuration of the S5-C interface, over which an

Setting	Description
Interface Settings	SGW-C instance communicates with a PGW-C instance in the network. These settings are described in SGW S5-C interface settings .
S5-u Interface Settings	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 settings are described in SGW S5-U interface settings .
S11 Interface Settings	These settings are described in SGW S11 interface settings .
DUT S11 Interface Settings	These settings are described in SGW DUT S11 interface settings .

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
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).
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.

Connectivity setting	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 <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.

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	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).
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.

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-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
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 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
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</i>

Connectivity setting	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.

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	347
SMF/PGW-C Range settings	348
SMF node settings	349
SMF N4 interface settings	350
SMF Nsmf interface settings	351
SMF S5-c interface settings	352
SMF remote SBA nodes	353
SMF Uplink Paths	357

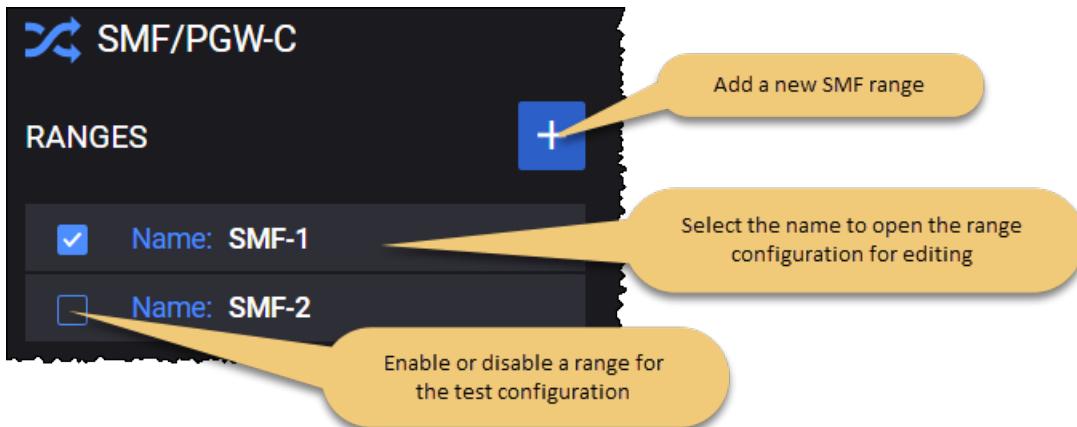
SMF/PGW-C Ranges panel

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 .
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 .
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 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 .

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

Slice and UPF Mapping

The following table describes the Slice and UPF Mapping settings.

Setting	Description
SMF NSSAI:	
	Select the Add NSSAI button to add a NSSAI to your test configuration.
SMF NSSAI:	
	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.
Uplink Path	Select the uplink path from the drop-down list. Default value: Default .

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.
Include 3GPP Interface Type	Select this check box to include the 3GPP interface type in PFCP messages.
Peer UPF	Select the UPF node connected to SMF over the N4 interface. Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific peer UPF node.

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 the node.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	
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
<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

Connectivity Settings	Description
	bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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 S5-c interface settings

The S5 interface provides user plane tunneling and tunnel management between Serving GW and PDN GW. It is used for Serving GW relocation due to UE mobility and if the Serving GW needs to connect to a non-collocated PDN GW for the required PDN connectivity.

You can enable or disable the S5-c interface, as required by your test configuration. For example:



S5-c Interface Settings

The following **Connectivity Settings** are required for the S5-c 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
<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	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.

SMF remote SBA nodes

AMF Connection Settings

Setting	Description
<i>AMF Connectivity Settings:</i>	
Peer AMF Type	Select one of the available options: <ul style="list-style-type: none"> • Preset • Discover More details below .
Indirect Communication without Delegated Discovery	IMPORTANT This option is visible only when SCP is selected in SCP Connection Settings. Select the option to enable it. For more details, refer to Indirect Communication without Delegated Discovery .

Setting	Description
Indirect Communication with Delegated Discovery	<p>IMPORTANT This option is visible only when Peer AMF Type is set to Discover and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to Indirect Communication with Delegated Discovery.</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](#) 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>	
Use SBI Fuzzing	<p>Use the toggle button to enable this option.</p> <p>When enabled, the <i>Peer UDM</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.</p>
SBI Fuzzer	Select the node from the drop-down list.

Setting	Description
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 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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer PCF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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 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>	
Use SBI	Use the toggle button to enable this option.

Setting	Description
Fuzzing	When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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, new options will be available:

- **Indirect Communication without Delegated Discovery** or
- **Indirect Communication with Delegated Discovery**

If Indirect Communication with or without Delegated Discovery option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which this option is enabled will be forwarded to the SCP. In the case of Indirect Communication with Delegated Discovery, SCP will also perform delegated discovery.

SEPP Connection Settings

To connect to the Security Edge Protection Proxy (SEPP) node, the following configuration settings are required.

Setting	Description
<i>SEPP Connection Settings:</i>	
Peer SEPP	Select either the IP address of a SCP node from your test network or <i>None</i> if you are not using one in your test configuration.
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.
Sepp Communication Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Telescopic FQDN • Target API Root

Home PLMN for Inter-PLMN Routing

The following configuration settings are required.

PLMN MCC	<p>Provide the PLMN MCC value.</p> <p><i>About PLMN MCC ...</i></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>Provide the PLMN MNC value.</p> <p><i>About PLMN MNC ...</i></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>

SMF Uplink Paths

Uplink Path settings

The following table describes the settings required to configure the uplink paths.

Setting	Description
<i>Uplink Paths:</i>	

Setting	Description
	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.

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	359
SMSF Range panel	359
SMSF node settings	360
SMSF Nsmsf interface settings	361
SMSF Remote SBA Nodes	362

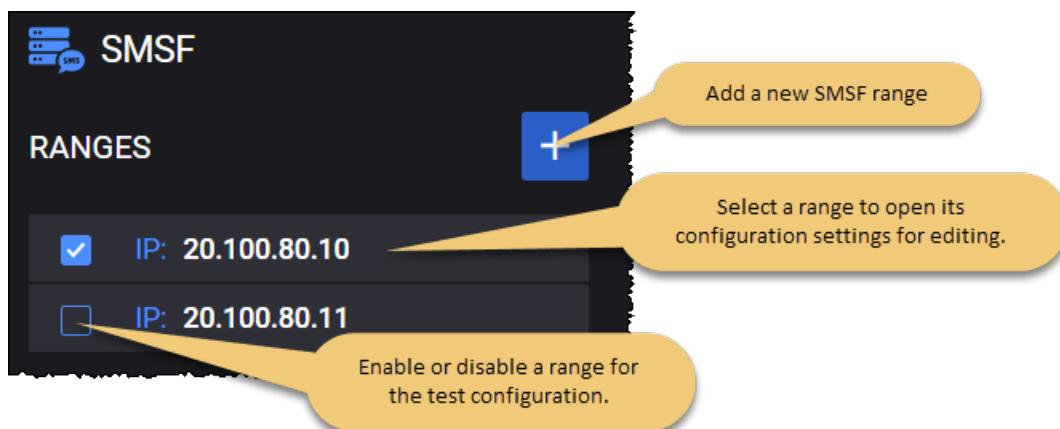
SMSF Ranges panel

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	Each SMSF range the configuration of an associated set of Node Settings, which are described in SMSF node settings .
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 .
Remote SBA Nodes	These settings are described in SMSF remote SBA nodes .

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
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).
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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>

Connectivity Settings	Description
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.
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

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	365
UDM/HSS Range panel	366
UDM Range Settings	366
UDM Settings	367
UDM Node Settings	368
UDM Nudm Interface Settings	370
UDM Remote SBA Nodes	371
HSS Range Settings	373
HSS Settings	374
HSS Node Settings	375
HSS S6a Interface Settings	375
UDM and HSS Range Settings	376

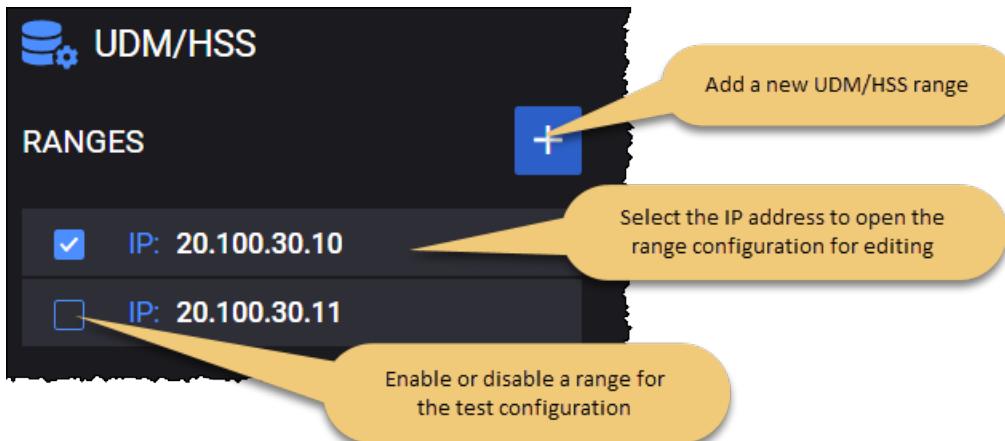
UDM/HSS Ranges panel

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/HSS, 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 enable the node and then configure it alongside with the connectivity settings required for the 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 selected node is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the selected node functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Enabled Nodes	This option allows you to enable a specific node (UDM , HSS or UDM and HSS) by selecting it from the drop-down list. Each node has specific range settings that need to be configured, as follows: <ul style="list-style-type: none"> • UDM Range Settings • HSS Range Settings • UDM and HSS Settings

UDM Range Settings

The following table describes the available **Range** configuration options for the UDM node.

Setting	Description
Settings	Each UDM range requires the configuration of an associated set of Settings, which are described in UDM settings .
UDM Node Settings	Each UDM range requires the configuration of an associated set of Node Settings, which are described in UDM node settings .
Nudm Interface	Each UDM range requires the configuration of Nudm interface settings, through which a UDM instance enables connectivity and interaction with other functions in the

Setting	Description
Settings	5G network. These settings are described in UDM Nudm interface settings .
Remote SBA Nodes	The remote SBA node settings are described in Remote SBA nodes .

UDM Settings

Each UDM instance requires the configuration of the following settings.

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>
<p><i>Network Initiated Deregistration:</i> You can enable or disable this option, as required by your test configuration.</p>	
Delay	Set the delay value.
Trigger	<p>Describes what triggers the sending of the Network Deregistration message.</p> <p>Available options:</p> <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	<p>Select the deregistration reason from the drop-down list. Available options:</p> <ul style="list-style-type: none"> • UE INITIAL REGISTRATION • UE REGISTRATION AREA CHANGE • SUBSCRIPTION WITHDRAWN

Setting	Description
	<ul style="list-style-type: none"> • 5GS TO EPS MOBILITY • 5GS TO EPS MOBILITY UE INITIAL REGISTRATION • REREGISTRATION REQUIRED

UDM Node Settings

Each UDM range includes a set of Node Settings plus one or more associated Routing Indicators. Also, here you can configure the SDM notifications 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.
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>

Routing Indicators: For details, refer to [Routing Indicators](#).

SDM Notifications: For details, refer to [SDM Notifications](#).

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.

Setting	Description
	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 remote 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 miliseconds) 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.

Setting	Description
<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. • 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> This represents the original path of the JSON object that has been moved.

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.

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.

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).
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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>	

Setting	Description
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

SEPP Connection Settings

To connect to the Security Edge Protection Proxy (SEPP) node, the following configuration settings are required.

Setting	Description
<i>SEPP Connection Settings:</i>	
Peer SEPP	Select either the IP address of a SCP node from your test network or <i>None</i> if you are not using one in your test configuration.
Protocol	The protocol to use for communication via SCP. It can be either HTTP or HTTPS.

Setting	Description
Port	The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.
Sepp Communication Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Telescopic FQDN • Target API Root

Home PLMN for Inter-PLMN Routing

The following configuration settings are required.

PLMN MCC	<p>Provide the PLMN MCC value.</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>Provide the PLMN MNC value.</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>

HSS Range Settings

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

Setting	Description
Settings	Each HSS range requires the configuration of an associated set of Settings, which are described in HSS settings .
HSS Node Settings	Each HSS range requires the configuration of an associated set of Node Settings, which are described in HSS node settings .
S6a Interface Settings	Each HSS range requires the configuration of S6a interface settings, through which a HSS instance enables connectivity and interaction with other functions in the 5G network. These settings are described in HSS S6a interface settings .

HSS Settings

Each HSS instance requires the configuration of the following settings.

Setting	Description
PLMN MCC	<p>The PLMN MCC for this HSS 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 HSS 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>
<p><i>Network Initiated Deregistration: You can enable or disable this option, as required by your test configuration.</i></p>	
Delay	Set the delay value.
Trigger	<p>Describes what triggers the sending of the Network Deregistration message.</p> <p>Available options:</p> <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	<p>Select the deregistration reason from the drop-down list. Available options:</p> <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

HSS Node Settings

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

Setting	Description
<i>HSS S6a: You can enable or disable the S6a interface, as required by your test configuration.</i>	
Origin Host Prefix	Set the origin host prefix. Default value: host .
Origin Realm	Set the origin realm. Default value: keysight.com .
Destination Host	Set the destination host prefix.
Destination Realm	Set the destination realm.
<i>Cancel Location: You can enable or disable this option, as required by your test configuration.</i>	
Delay	Set the delay value.

HSS S6a Interface Settings

S6a is the service-based interface through which a HSS instance makes its services available to other services in a 5G network.

The following **Connectivity Settings** enable the necessary S6a 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).
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
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.

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.

UDM and HSS Range Settings

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

Setting	Description
Settings	Each UDM and HSS range requires the configuration of an associated set of Settings, which are described in UDM settings or HSS settings .
UDM Node Settings	Each UDM and HSS range requires the configuration of an associated set of UDM Node Settings, which are described in UDM node settings .
Nudm Interface Settings	Each UDM and HSS 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 Nudm interface Settings .
HSS Node Settings	Each UDM and HSS range requires the configuration of an associated set of HSS Node Settings, which are described in HSS node settings .
S6a Interface Settings	Each UDM and HSS range requires the configuration of S6a interface settings, through which a HSS instance enables connectivity and interaction with other functions in the 5G network. These settings are described in HSS S6a interface settings .
Remote SBA Nodes	The remote SBA node settings are described in remote SBA nodes .

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:

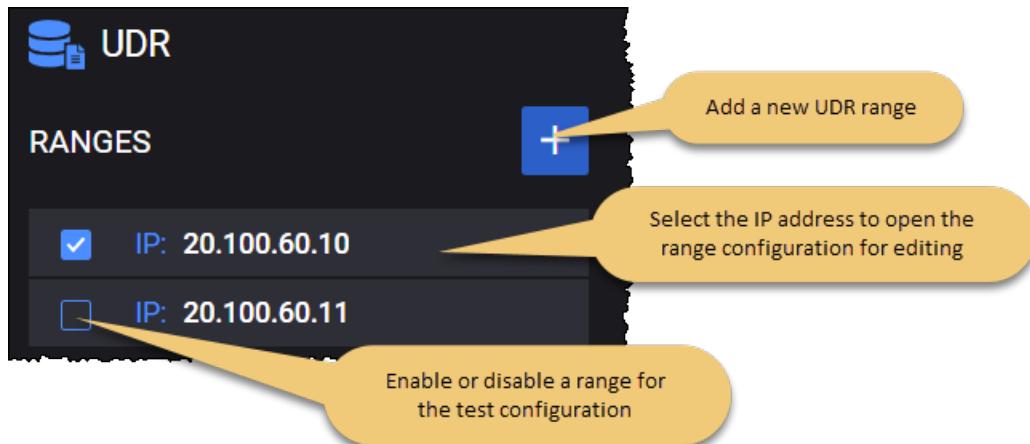
UDR Ranges panel	377
UDR Range panel	377
UDR Nudr interface settings	378
UDR Remote SBA Nodes	380

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	Each UDR range requires the configuration of an associated set of Node Settings, which are described in UDR node settings .
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 .
Remote SBA Nodes	The remote SBA node settings are described in UDR remote SBA nodes .

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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

UPF/PGW-U configuration settings



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	382
UPF/PGW-U Range panel	382
UPF N3 interface settings	383
UPF N4 interface settings	384
UPF N6 interface settings	386
UPF N9 interface settings	386

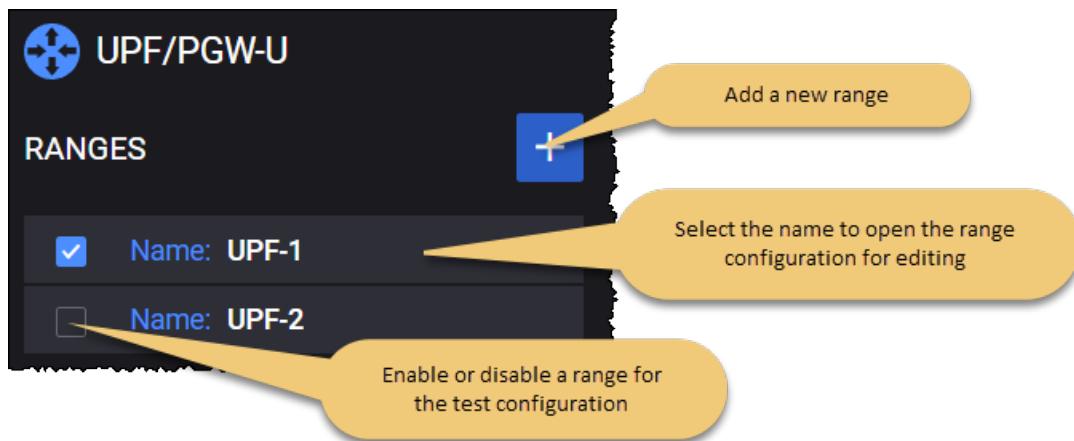
UPF/PGW-U Ranges panel

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).
Name	The name of the UPF range. You can accept the name provided by the LoadCore, or

Setting	Description
	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 .
N4 Interface Settings	N4 is the interface between the SMF and the UPF. These interface settings are described in UPF N4 interface settings .
N6 Interface Settings	N6 is the interface between the DN and the UPF. These interface settings are described in UPF N6 interface settings .
N9 Interface Settings	N9 is the interface between two UPFs. These interface settings are described in UPF N9 interface settings .

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>
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>
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>	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.
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.

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:

N9 Interface Settings

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>	<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 MAC Address). The default value is 000000000001.

Connectivity Settings	Description
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.

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	389
5G-EIR Range panel	389
5G-EIR node settings	390
5G-EIR N5g-eir interface settings	390
5G-EIR Remote SBA Nodes	392

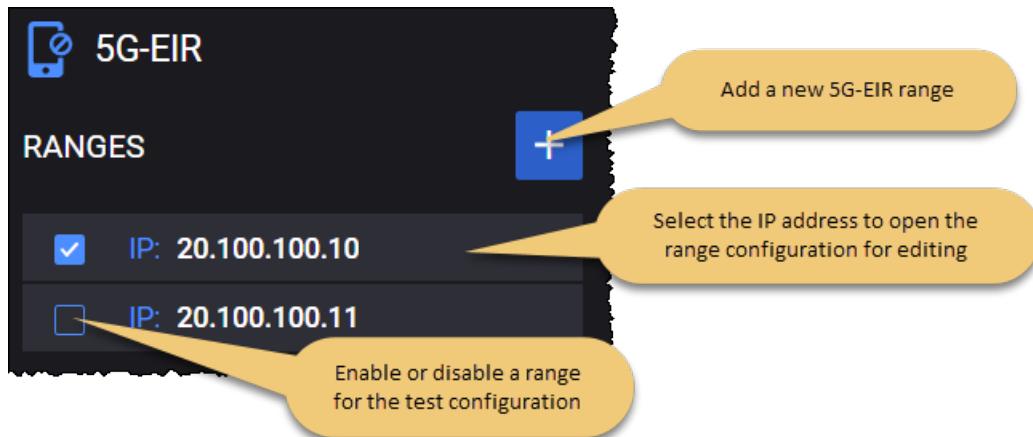
5G-EIR Ranges panel

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 .
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 .
Remote SBA Nodes	The remote SBA node settings are described in 5G-EIR remote SBA nodes .

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>	<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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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>	
Use SBI Fuzzing	Use the toggle button to enable this option. When enabled, the <i>Peer NRF</i> drop-down is hidden and a new drop-down called <i>SBI Fuzzer</i> is displayed.
SBI Fuzzer	Select the node from the drop-down list.
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.

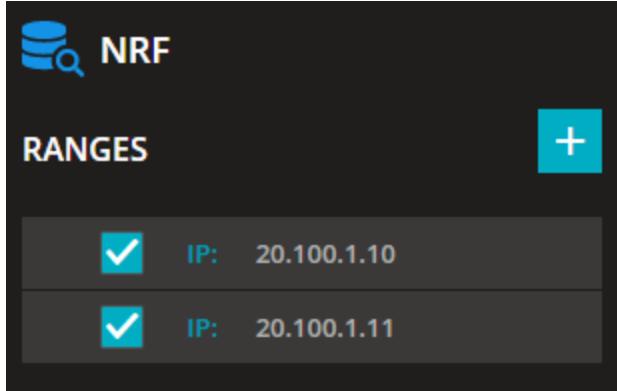
NF Discovery service

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.

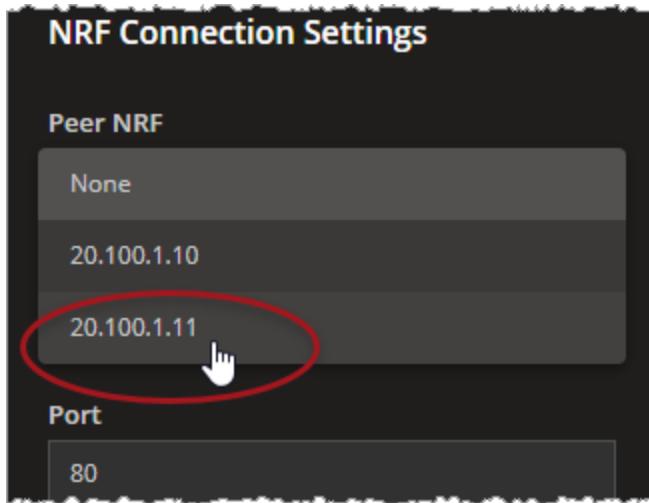
NF Discovery in LoadCore

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:

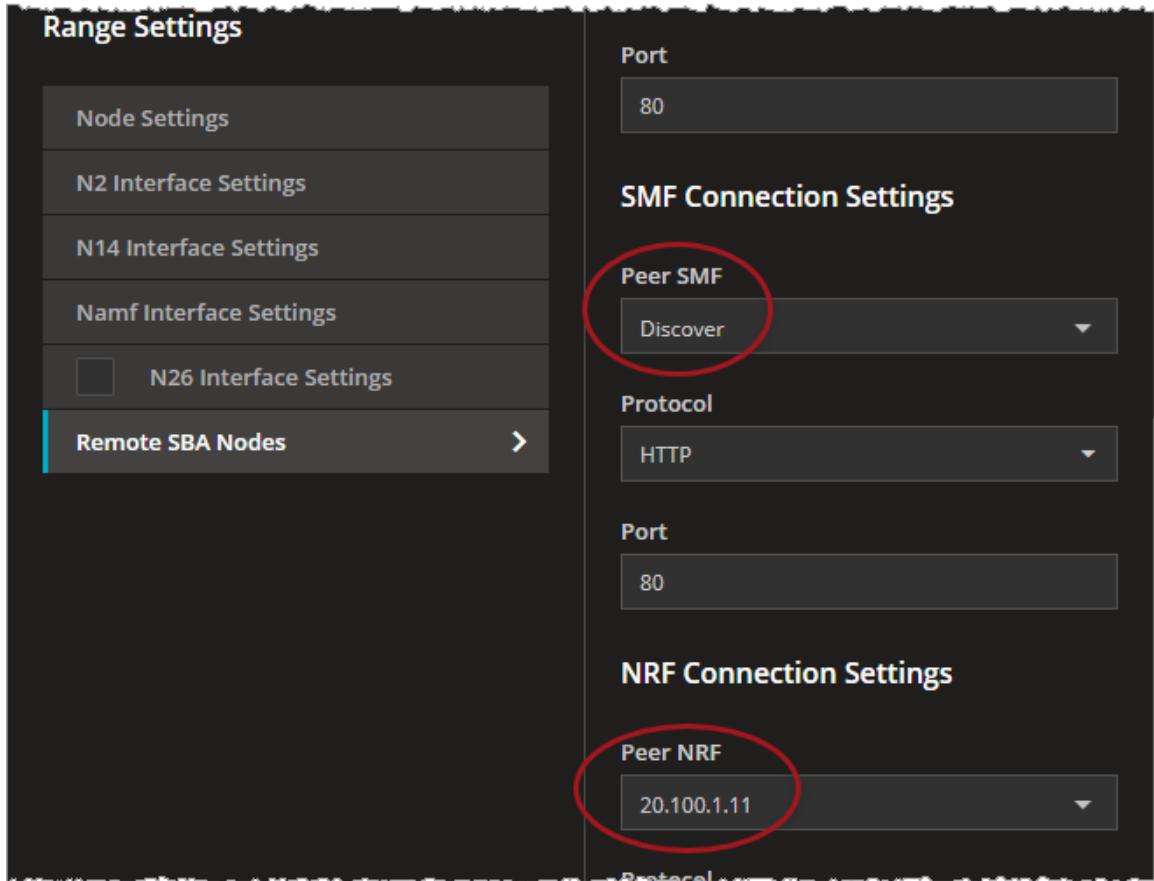


This is the NRF to which the node is registering.

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).

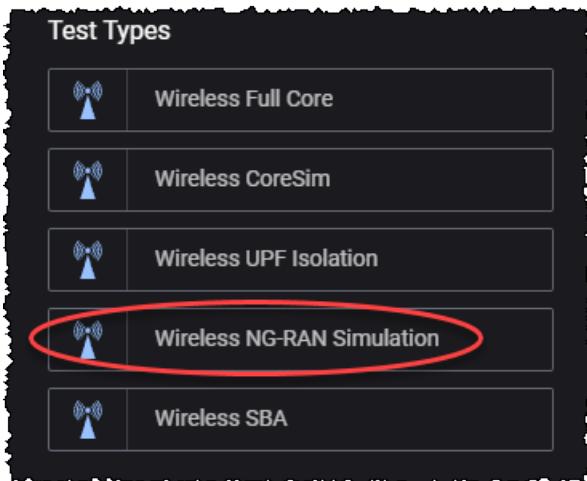
For example:



CHAPTER 8

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:

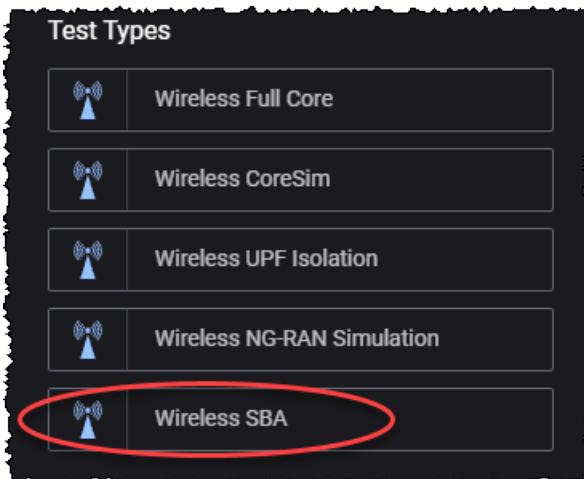
- The AMF and UPF nodes are configured as DUTs.
- The UE, RAN, and DN nodes are enabled for testing.
- All other simulated nodes are disabled by default.

For more details about configuring a Full Core test, refer to [Full Core tests: configuration settings](#).

CHAPTER 9

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	400
UE configuration settings	401
UE Ranges panel	402
UE Range panel	402
Range Settings	403
UE Identification	404
UE Security	405
UE Settings	407
UE SDF settings	408
Shared Data IDs	408
UE Subscribed AMBR settings	408
Service Area Restrictions	409
Forbidden Areas	410

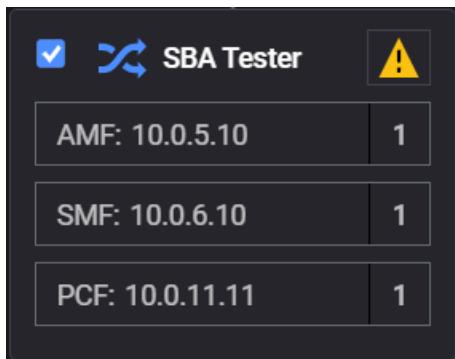
Notifications	411
Network Slicing	411
UDM Default NSSAI settings	413
UDM SNSSAI Mappings	413
UDR SNSSAI Settings	414
Charging Function	415
Converged Charging	415
Spending Limit Control	416
Objectives	419
Primary Objective	420
About primary objectives	421
Primary Objective Parameters	423
Secondary Objectives	439
UEGetNSSAIAMF2UDM	440
RegistrationAMF2UDM	441
DeregistrationAMF2UDM	442
GetPolicyAMF2PCF	443
UpdatePolicyAMF2PCF	444
GetPolicySMF2PCF	446
UpdatePolicySMF2PCF	447
RegistrationSMF2UDM	449
DeregistrationSMF2UDM	450
IntermediateSpendingLimitPCF2CHF	450
ConvergedChargingUpdateSMF2CHF	451
SBA Tester Global Settings panel	456
Connection Settings	457
Advanced Settings	457
Impairment	459
DNNs panel	460
DNN configuration settings	461
DNN GBR configuration settings	463
Session AMBR configuration settings	463

QoS Flows panel	464
QoS Flow configuration settings	465
QoS Flow Packet Filter configuration settings	467
QoS Flow Maximum Packet Loss configuration settings	468
QoS Flow ARP configuration settings	468
QoS Flow MBR configuration settings	469
QoS Flow GBR configuration settings	469
SBA Tester Simulated Nodes panel	470
AMF configuration settings	470
SMF configuration settings	476
PCF configuration settings	481
SBA Tester Remote SBA Nodes	487
SBA Tester Remote Nodes	489
AUSF configuration settings	491
AUSF Ranges panel	492
AUSF Range panel	492
AUSF node settings	493
AUSF Nausf interface settings	494
AUSF remote SBA nodes	495
CHF configuration settings	497
CHF Ranges panel	497
CHF Range panel	498
CHF node settings	498
CHF Nchf interface settings	499
CHF remote SBA nodes	500
NRF configuration settings	500
NRF Ranges panel	501
NRF Range panel	501
NRF node settings	502
NRF Nnrf interface settings	503
NSSF configuration settings	505
NSSF Ranges panel	506

NSSF Range panel	506
NSSF node settings	507
Nnssf Interface Settings	508
Remote SBA nodes	509
NSSF Restricted NSSAIs	510
NSSF Network Slices	511
NSSF Configured NSSAI	512
PCF configuration settings	513
PCF Ranges panel	513
PCF Range panel	513
PCF node settings	514
PCF service area restrictions	516
PCF Npcf interface settings	517
PCF remote SBA nodes	518
SCP configuration settings	519
SCP Ranges panel	519
SCP Range panel	520
SCP Nscp interface settings	521
SCP Remote SBA Nodes	522
UDM configuration settings	523
UDM Ranges panel	523
UDM Range panel	524
UDM node settings	524
UDM Nudm interface settings	527
UDM remote SBA nodes	529
UDR configuration settings	529
UDR Ranges panel	530
UDR Range panel	530
UDR Nudr interface settings	531
UDR remote SBA nodes	532

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.

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:

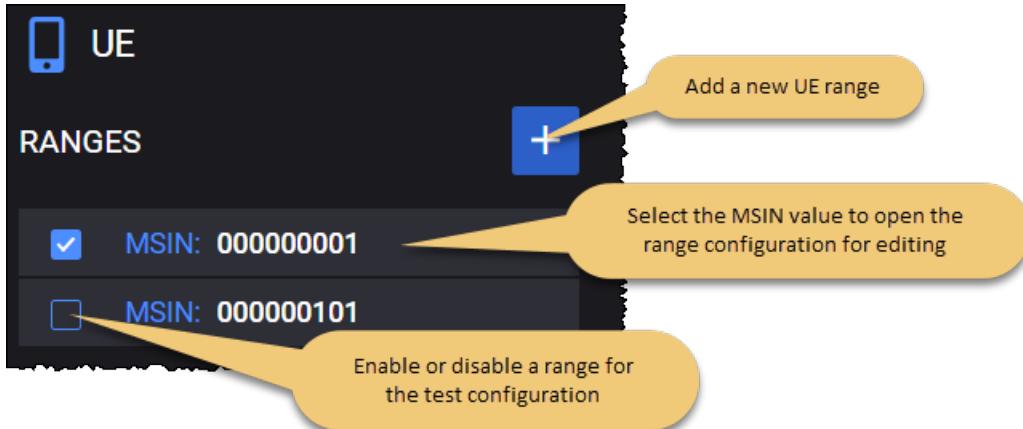
UE Ranges panel	402
UE Range panel	402
Range Settings	403
UE Identification	404
UE Security	405
UE Settings	407
UE SDF settings	408
Shared Data IDs	408
UE Subscribed AMBR settings	408
Service Area Restrictions	409
Forbidden Areas	410
Notifications	411
Network Slicing	411
UDM Default NSSAI settings	413
UDM SNSSAI Mappings	413
UDR SNSSAI Settings	414
Charging Function	415
Converged Charging	415
Spending Limit Control	416

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](#)
- [Network Slicing](#)
- [Test Objectives](#)

Range Settings

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

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

- [UE Identification](#)
- [UE Security](#)
- [UE Settings](#)
- [UE SDF settings](#)
- [Shared Data IDs](#)
- [UE Subscribed AMBR settings](#)
- [Service Area Restrictions](#)
- [Forbidden Areas](#)

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	<p>The IMEI value that will be assigned to the first simulated UE in the range.</p> <p>The International Mobile Equipment Identity (IMEI) is a number used to uniquely identify 3GPP and iDEN mobile phones, as well as some satellite phones. It identifies the origin, model, and serial number of the device. It consists of either 15 digits (14 digits plus one check digit); or 16 digits (14 digits plus two software version digits). GSM networks use the IMEI number to identify valid devices, and can also use the number to prevent a stolen phone from accessing the network.</p> <p>When it includes the software version digits, it is referred to as the IMEISV.</p>
IMEI Increment	The value to use for incrementing the IMEI values for each of the UEs in the range.
Software Version	The software version number identifies the software version number of the mobile equipment. Its length is 2 digits.
MSISDN	The first Mobile Station ISDN (MSISDN) value for this range.
MSISDN Increment	The value to use for incrementing the MSISDNs in the range.
UE 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	The value to use for incrementing the IPv6 address prefixes for each of the UEs in the range.

Setting	Description
Prefix Increment	
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 / OPc / TOP / TOPc	Select the operator-specific authentication value.
OP	The Auth OP value specifies the operator-specific authentication value to use for the UEs in this range. It is a string with a maximum length of 34 characters. It remains fix for all Subscriber/SIM of an operator. You can accept the value generated by 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.

Setting	Description												
OPc Increment	The number used to increment the OPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same OPc value.												
TOP	A 256-bit operator variant algorithm configuration field used by the TUAK authentication algorithm.												
TOPc	A 256-bit value derived from TOP and K used by the TUAK authentication algorithm.												
TOPc Increment	The number used to increment the TOPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same TOPc value.												
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	<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 Public Key	The home network public key that will be use for concealing the SUPI. The USIM stores the home network public key (if provisioned by the home operator).												
Home Network Public Key ID	The Home Network Public Key Identifier that will be used to indicate which public/private key pair to use for SUPI protection and deconcealment of the SUCI.												
Ephemeral Public Key	The ephemeral public key that will be used for computing a fresh SUCI on the UE side and for deconcealing the SUCI on the home network side.												
Ephemeral Private Key	The ephemeral private key that will be used for computing a fresh SUCI on the UE side.												
Routing Indicator	The Routing Indicator that is used in the construction of the SUCI.												

Setting	Description
	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 Timer	The Periodic Registration timer value for this range of UEs. The AMF allocates a periodic registration timer value to the UE based on local policies, subscription information and information provided by the UE. After the expiry of this timer, the UE performs a periodic registration.
Active Time	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. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.
Subscribed AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.

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

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.

Use the settings described below to configure service area restrictions for a UE range. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.

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>	

Setting	Description
	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 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.

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</p>

Setting	Description
	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).

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 (ms)	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 notification	Enable subscription to application data notifications for the UE range.
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	413
UDM SNSSAI Mappings	413

UDR SNSSAI Settings **414**

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 NSSAI slices are the ones supported and requested 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 **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 configured 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>	

Setting	Description
	Select the Delete SNSSAI Mapping button to delete this NSSAI mapping from your test configuration.
SST	The Slice/Service Type (SST) value.
SD	The Slice Differentiator (SD) value for this S-NSSAI.
Mapped SST	The Mapped Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The Mapped Slice Differentiator (SD) value for this S-NSSAI.
DNNS	The Subscription Information for each S-NSSAI may contain a Subscribed DNN list. Select one or more DNNs from the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .

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 .

Charging Function

LoadCore's Charging Function supports Converged Charging and Spending Limit Control functionalities.

Converged Charging is a process where online and offline charging are combined. The charging information is utilized by CCS(Converged Charging System) in one converged charging service which offers charging with and without quota management, as well as charging information record generation.

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.

Converged Charging

The following table describes the UE **Converged Charging** settings.

Setting	Description
Validity Time	The validity of the granted quota for a given category instance.
Quota Holding Time	A quota expiry time, when no traffic associated with the quota is observed for the value indicated by this attribute.
Time Quota Threshold	A time quota below this threshold will trigger a quota re-authorization.
Volume Quota Threshold	A volume quota below this threshold will trigger a quota re-authorization.
Unit Quota Threshold	A units quota below this threshold will trigger a quota re-authorization.
Notification Timer	Duration in milliseconds after which the CHF will notify CTF about quota re-authorization.
Enable Subscription Termination Timer	Select this option to enable the subscription termination timer.
<i>Total Available Units Per PDU Session:</i>	<i>Holds the maximum amount of units to be granted per PDU session per charging session.</i>
Total Time	Set the total time value.
Total Volume	Set the total volume value.
Total Uplink Volume	Set the total uplink volume value.
Total Downlink Volume	Set the total downlink volume value.
Total Service Specified Units	Set the total service specified units value.

Setting	Description
<i>Default Granted Units Per Charging Data Request:</i>	
Time	Set the time value.
Volume	Set the volume value.
Uplink Volume	Set the uplink volume value.
Downlink Volume	Set the downlink volume value.
Service Specified Units	Set the service specified units value.

Spending Limit Control

The following table describes the UE **Spending Limit Control** settings.

Setting	Description
Enable Notify Timer	Use this option to enable 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	Use this option to enable 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	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.
<i>Policy Counters</i>	<i>These settings are described here.</i>
<i>Notify Policy Counters</i>	<i>These settings are described here.</i>

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.
<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>	

Setting	Description
	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 Counter Status	Enter the policy counter status (as a string value). For example: <i>120Mbps</i> .
Activation Time	Enter the activation time (as a DateTime value) for this status value. For example: <i>2020-12-31 11:59:59</i> .

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	420
About primary objectives	421
Primary Objective Parameters	423
Secondary Objectives	439
UEGetNSSAIAMF2UDM	440
RegistrationAMF2UDM	441
DeregistrationAMF2UDM	442
GetPolicyAMF2PCF	443
UpdatePolicyAMF2PCF	444
GetPolicySMF2PCF	446
UpdatePolicySMF2PCF	447
RegistrationSMF2UDM	449
DeregistrationSMF2UDM	450
IntermediateSpendingLimitPCF2CHF	450
ConvergedChargingUpdateSMF2CHF	451

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.

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

Active Subscribers

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

<i>Ramp Up Time:</i>	20000 / 1000 = 20s for subscribers to register
<i>Rate in ramp up time:</i>	1000 registrations per second

<i>Sustain time:</i>	30 seconds
<i>Rate in sustain time:</i>	2000 secondary procedures per second
<i>Ramp down time:</i>	$20000 / 1000 = 20\text{s}$ 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 Objective Parameters

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
Procedure Type	Select the procedure type from the drop-down list: <ul style="list-style-type: none"> • UE Authentication Request AMF to AUSF • Create Policy AMF to PCF • Create Policy SMF to PCF • Initial Spending Limit PCF to CHF • Converged Charging SMF to CHF
Objective Type	Select the desired Primary Objective Type: <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. The panel will display the settings for the selected Objective Type.
<i>Active Subscribers:</i>	
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 after NG-Setup/S1-Setup have successfully completed.
<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	The duration of time (in Seconds) that the specified session activation rate will be

Parameter	Description
(s)	maintained.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.

UE Authentication Request AMF to AUSF

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.
User Location	Select NR Location to open the configuration panel for these settings, which are describde below in User Location .

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).
- Global RAN Node Id settings

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.
UE Location Timestamp	The timestamp 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.
<i>Global Ran Node Id:</i>	
MCC	Set the mobile country code.
MNC	Set the mobile network code.
N3 Iwf Id	Set the value for this field.
Bit Length	Set the bit length value.
GNB value	Set the GNB value.
Nge Nb Id	Set the value for this field.

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 .
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 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

Procedure setting	Description
	hexadecimal string that indicates the features supported (as described in TS 29.571).
<i>QoS Settings</i>	Select QoS Settings to open the configuration panel for these settings, which are described below in QoS Settings .
<i>User Location</i>	Select NR Location to open the configuration panel for these settings, which are described below in User Location .

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	Specify the 5QI value (decimal number) to use for this procedure. 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.
ARP:	
ARP Priority Level	Specify the ARP priority level to use for this procedure. 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.
ARP Preemption Capability	Select Not Preemp or May Preempt . When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.
ARP Preemption Vulnerability	Select Not Preemptable or Preemptable . 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.

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).
- Global RAN Node Id settings

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.
UE Location Timestamp	The timestamp 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.
<i>Global Ran Node Id:</i>	
MCC	Set the mobile country code.
MNC	Set the mobile network code.

Parameter	Description
N3 Iwf Id	Set the value for this field.
Bit Length	Set the bit length value.
GNB value	Set the GNB value.
Nge Nb Id	Set the value for this field.

Initial Spending Limit PCF to CHF

The following table describes the settings for the **Initial Spending Limit PCF to CHF** Procedure.

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.

Converged Charging SMF to CHF

The following table describes the configuration settings for the **Converged Charging SMF to CHF** procedure.

Parameter	Description
<i>PDU Session Information:</i>	
RAT Type	Select the RAT type value to use for this policy association. The options available in LoadCore are: NR , EUTRA , WLAN , and VIRTUAL . The RAT Type attribute indicates where the served UE is camping.
DNN	Select one of the configured DNNs from the drop-down list.
Charging Characteristics	Set the charging characteristics value.

Parameter	Description
Charging Characteristics Selection Mode	Select the charging characteristics mode from the drop-down list: <ul style="list-style-type: none">• HOME_DEFAULT• ROAMING_DEFAULT• VISITING_DEFAULT
Amfld	Set the value for this field.
PDU Address	Select PDU Address to open the configuration panel for these settings, which are described below in PDU Address .
Subscriber Settings	Select Subscriber Settings to open the configuration panel for these settings, which are described below in Subscriber Settings .
Authorized Settings	Select Authorized Settings to open the configuration panel for these settings, which are described below in Authorized Settings .
User Location Information	Select User Location Information to open the configuration panel for these settings, which are described below in User Location Information .
Ratings Groups	The Ratings Groups settings are described below in Ratings Groups .

PDU Address

These configuration settings are described in the following table.

Parameter	Description
IP Address	Provide the IP address.
IPv6 Address Prefix	Set the IPv6 address prefix.
IP Address Prefix Length	Set the length of the IP address prefix.
IPv4 Dynamic Address Flag	Enable or disable this option based on your test requirements.
IPv6 Dynamic Prefix Flag	Enable or disable this option based on your test requirements.

Subscriber Settings

These configuration settings are described in the following table.

Parameter	Description
<i>QoS Settings: Select QoS Settings to open the configuration panel for these settings.</i>	
QoS Settings	
Priority Level	Specify the priority level.

Parameter	Description
5QI	Specify the 5QI value (decimal number) to use.
ARP	
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 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>
<i>Session AMBR: Select Session AMBR to open the configuration panel for these settings.</i>	
Subscribed Session AMBR Uplink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Subscribed Session AMBR Downlink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink rate.

Authorized Settings

These configuration settings are described in the following table.

Parameter	Description
<i>QoS Settings: Select QoS Settings to open the configuration panel for these settings.</i>	
QoS Settings	
AverWindow	Specify the averaging window value. It represents the time duration (specified in milliseconds) over which the GFBR and MFBR are calculated.
MaxDataBurstVol	Specify the maximum data burst volume.
maxbrUI	Set the maximum bit rate value for uplink traffic.
maxbrDI	Set the maximum bit rate value for downlink traffic.

Parameter	Description
gbrUl	Set the guaranteed bit rate value for uplink traffic.
gbrDl	Set the guaranteed bit rate value for downlink traffic.
qnc	Enable or disable the QoS Notification Control parameter.
Priority level	Specify the priority level.
5QI	Specify the 5QI value (decimal number) to use.
ARP	
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 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>
<i>Session AMBR: Select Session AMBR to open the configuration panel for these settings.</i>	
Subscribed Session AMBR Uplink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Subscribed Session AMBR Downlink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink rate.

User Location Information

These configuration settings are described in the following table.

Parameter	Description
<i>NR Location: Select NR Location to open the configuration panel for these settings.</i>	
NR Location	
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.
UE Location Timestamp	The timestamp 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.
<i>Global Ran Node Id</i>	
MCC	Set the mobile country code.
MNC	Set the mobile network code.
N3 Iwf Id	Set the value for this field.
Bit Length	Set the bit length value.
GNB value	Set the GNB value.
Nge Nb Id	Set the value for this field.
<i>EUTRA Location: Select EUTRA Location to open the configuration panel for these settings.</i>	
<i>EUTRA 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.

Parameter	Description
Geodetic information	The Geodetic Location value that the procedure will use in the identification of the UE location.
UE Location Timestamp	The timestamp 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>ECGI</i>	
MCC	The PLMN MCC that is used in the construction of this ECGI.
MNC	The PLMN MNC that is used in the construction of this ECGI.
EUTRA Cell ID	The EUTRA Cell ID that is used in the construction of this ECGI.
<i>Global Ran Node Id</i>	
MCC	Set the mobile country code.
MNC	Set the mobile network code.
N3 Iwf Id	Set the value for this field.
Bit Length	Set the bit length value.
GNB value	Set the GNB value.
Nge Nb Id	Set the value for this field.
<i>N3GA Location: Select N3GA Location to open the configuration panel for these settings.</i>	
<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.
N3 Iwf Id	Set the value for this field.
UE IPV4 Address	Set the UE IPV4 address.

Parameter	Description
UE IPV6 Address	Set the UE IPV6 address.
Port Number	Set the port number.

Rating Groups

The following table describes the Rating Groups settings.

Parameter	Description
	Select the Add Group button to add a new rating group to your test configuration.
<i>Rating Group</i>	
	Select this button to remove the rating group from your test configuration.
Id	Set the Id value for this rating group.
UPF Id	Set the UPF Id value for this rating group.
<i>Requested Unit</i>	
Time	Set the total time value.
Total Volume	Set the total volume value.
Uplink Volume	Set the total uplink volume value.
Downlink Volume	Set the total downlink volume value.
Service Specific Units	Set the total service specified units value.
<i>Used Units</i>	
	Select the Add unit button to add a new unit to your test configuration.
	Select this button to remove this unit from your test configuration.
Service Id	Set the service Id.
Quota Management Indicator	Select an option from the drop-down list: <ul style="list-style-type: none"> • ONLINE_CHARGING • OFFLINE_CHARGING
Time	Set the total time value.

Parameter	Description
Total Volume	Set the total volume value.
Uplink Volume	Set the total uplink volume value.
Downlink Volume	Set the total downlink volume value.
Service Specific Units	Set the total service specified units value.
Charging Rule Base Name	Set the name of the charging rule
3GPPPS Data Off Status	Select an option from the drop-down list: <ul style="list-style-type: none"> • INACTIVE • ACTIVE
Sponsor Identity	Specify the sponsor identity.
Application Service Provider Identity	Specify the application service provider.
Service Specific Units	Set the service specific units value.
<i>QoS Information</i>	Select QoS Information to open the configuration panel for these settings, which are described below in QoS Information .
<i>Triggers</i>	The Triggers settings are described below in Triggers .

The following table describes the QoS Information settings.

Parameter	Description
QoS Id	Specify the QoS id.
AverWindow	Specify the averaging window value. It represents the time duration (specified in milliseconds) over which the GFBR and MFBR are calculated.
MaxDataBurstVol	Specify the maximum data burst volume.
maxbrUI	Set the maximum bit rate value for uplink traffic.
maxbrDI	Set the maximum bit rate value for downlink traffic.
gbrUI	Set the guaranteed bit rate value for uplink traffic.
gbrDI	Set the guaranteed bit rate value for downlink traffic.
qnc	Enable or disable the QoS Notification Control parameter.
Priority level	Specify the priority level.

Parameter	Description
Reflective Qos	Enable or disable reflective QoS.
Sharing Key Download	Specify the sharing key used for download.
Sharing Key Upload	Specify the sharing key used for upload.
Max Packet Loss Rate Download	The maximum download packet loss rate (packets per second) that is permitted for the QoS Flow.
Max Packet Loss Rate Upload	The maximum upload packet loss rate (packets per second) that is permitted for the QoS Flow.
Def Qos Flow Indication	Enable or disable this option.
5QI	Specify the 5QI value (decimal number) to use for this procedure.
ARP	
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 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>

The following table describes the Triggers settings.

Parameter	Description
	Select the Add Trigger button to add a new trigger to your test configuration.
<i>Trigger</i>	
	Select this button to remove this trigger from your test configuration.

Parameter	Description
Trigger Type	Select an option from the drop-down list: UOTA_THRESHOLD, QHT, FINAL, QUOTA_EXHAUSTED, VALIDITY_TIME, OTHER_QUOTA_TYPE, FORCEDREAUTHORISATION, UNUSED_QUOTA_TIMER, UNIT_COUNT_INACTIVITY_TIMER, ABNORMAL_RELEASE, QOS_CHANGE, VOLUME_LIMIT, TIME_LIMIT, PLMN_CHANGE, USER_LOCATION_CHANGE, RAT_CHANGE, UE_TIMEZONE_CHANGE, TARIFF_TIME_CHANGE, MAX_NUMBER_OF_CHANGES_IN_CHARGING_CONDITIONS, MANAGEMENT_INTERVENTION, CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA, CHANGE_OF_3GPP_PS_DATA_OFF_STATUS, SERVING_NODE_CHANGE, REMOVAL_OF_UPF, ADDITION_OF_UPF, START_OF_SERVICE_DATA_FLOW
Trigger Category	Select an option from the drop-down list: <ul style="list-style-type: none"> • IMMEDIATE_REPORT • DEFERRED_REPORT
Time Limit	Specify the time limit.
Volume Limit 64	Specify the volume limit.
Max Number of ccc	Set the value for this field.

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	440
RegistrationAMF2UDM	441
DeregistrationAMF2UDM	442
GetPolicyAMF2PCF	443
UpdatePolicyAMF2PCF	444
GetPolicySMF2PCF	446
UpdatePolicySMF2PCF	447
RegistrationSMF2UDM	449
DeregistrationSMF2UDM	450
IntermediateSpendingLimitPCF2CHF	450
ConvergedChargingUpdateSMF2CHF	451

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 start 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.

ConvergedChargingUpdateSMF2CHF

The following table describes the **Settings** for the *ConvergedChargingUpdateSMF2CHF* Secondary Objective.

Parameter	Description
	Select the Delete Objective button to delete this Secondary Objective from your test configuration.
Procedure	Converged Charging Update SMF to CHF.
Iterations	The number of times the procedure will run. It can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.

Parameter	Description
Distributed over (s)	Set the value for this field.
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>Converged Charging Update SMF to CHF</i>	
Maximum Updates	Set the number of maximum updates.
Delay Between Updates	Set the value of the delay between updates.
Rating Groups	<i>The required setting are described below.</i>

Rating Groups

The following table describes the Rating Groups settings.

Parameter	Description
	Select the Add Group button to add a new rating group to your test configuration.
<i>Rating Group</i>	
	Select this button to remove the rating group from your test configuration.
Id	Set the Id value for this rating group.
UPF Id	Set the UPF Id value for this rating group.
<i>Requested Unit</i>	
Time	Set the total time value.
Total Volume	Set the total volume value.
Uplink Volume	Set the total uplink volume value.
Downlink Volume	Set the total downlink volume value.
Service Specific Units	Set the total service specified units value.

Parameter	Description
<i>Used Units</i>	
	Select the Add unit button to add a new unit to your test configuration.
	Select this button to remove this unit from your test configuration.
Service Id	Set the service Id.
Quota Management Indicator	Select an option from the drop-down list: <ul style="list-style-type: none"> • ONLINE_CHARGING • OFFLINE_CHARGING
Time	Set the total time value.
Total Volume	Set the total volume value.
Uplink Volume	Set the total uplink volume value.
Downlink Volume	Set the total downlink volume value.
Service Specific Units	Set the total service specified units value.
Charging Rule Base Name	Set the name of the charging rule
3GPPPS Data Off Status	Select an option from the drop-down list: <ul style="list-style-type: none"> • INACTIVE • ACTIVE
Sponsor Identity	Specify the sponsor identity.
Application Service Provider Identity	Specify the application service provider.
Service Specific Units	Set the service specific units value.
QoS Information	Select QoS Information to open the configuration panel for these settings, which are described below in QoS Information .
Triggers	The Triggers settings are described below in Triggers .

QoS Information

The following table describes the QoS Information settings.

Parameter	Description
QoS Id	Specify the QoS id.

Parameter	Description
AverWindow	Specify the averaging window value. It represents the time duration (specified in milliseconds) over which the GFBR and MFBR are calculated.
MaxDataBurstVol	Specify the maximum data burst volume.
maxbrUI	Set the maximum bit rate value for uplink traffic.
maxbrDI	Set the maximum bit rate value for downlink traffic.
gbrUI	Set the guaranteed bit rate value for uplink traffic.
gbrDI	Set the guaranteed bit rate value for downlink traffic.
qnc	Enable or disable the QoS Notification Control parameter.
Priority level	Specify the priority level.
Reflective Qos	Enable or disable reflective QoS.
Sharing Key Download	Specify the sharing key used for download.
Sharing Key Upload	Specify the sharing key used for upload.
Max Packet Loss Rate Download	The maximum download packet loss rate (packets per second) that is permitted for the QoS Flow.
Max Packet Loss Rate Upload	The maximum upload packet loss rate (packets per second) that is permitted for the QoS Flow.
Def Qos Flow Indication	Enable or disable this option.
5QI	Specify the 5QI value (decimal number) to use for this procedure.
ARP	
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 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>

Parameter	Description
ARP Preemption Vulnerability	Select Not Preemptable or Preemptable . 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.

Triggers

The following table describes the Triggers settings.

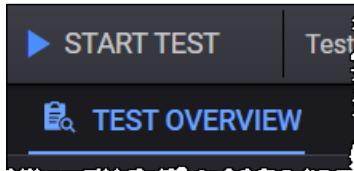
Parameter	Description
	Select the Add Trigger button to add a new trigger to your test configuration.
<i>Trigger</i>	
	Select this button to remove this trigger from your test configuration.
Trigger Type	Select an option from the drop-down list: UOTA_THRESHOLD, QHT, FINAL, QUOTA_EXHAUSTED, VALIDITY_TIME, OTHER_QUOTA_TYPE, FORCEDREAUTHORISATION, UNUSED_QUOTA_TIMER, UNIT_COUNT_INACTIVITY_TIMER, ABNORMAL_RELEASE, QOS_CHANGE, VOLUME_LIMIT, TIME_LIMIT, PLMN_CHANGE, USER_LOCATION_CHANGE, RAT_CHANGE, UE_TIMEZONE_CHANGE, TARIFF_TIME_CHANGE, MAX_NUMBER_OF_CHANGES_IN_CHARGING_CONDITIONS, MANAGEMENT_INTERVENTION, CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA, CHANGE_OF_3GPP_PS_DATA_OFF_STATUS, SERVING_NODE_CHANGE, REMOVAL_OF_UPF, ADDITION_OF_UPF, START_OF_SERVICE_DATA_FLOW
Trigger Category	Select an option from the drop-down list: <ul style="list-style-type: none"> • IMMEDIATE_REPORT • DEFERRED_REPORT
Time Limit	Specify the time limit.
Volume Limit 64	Specify the volume limit.
Max Number of ccc	Set the value for this field.

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 **457**

Advanced Settings **457**

Impairment **459**

DNNs panel **460**

 DNN configuration settings 461

 DNN GBR configuration settings 463

 Session AMBR configuration settings 463

QoS Flows panel **464**

 QoS Flow configuration settings 465

 QoS Flow Packet Filter configuration settings 467

 QoS Flow Maximum Packet Loss configuration settings 468

 QoS Flow ARP configuration settings 468

 QoS Flow MBR configuration settings 469

 QoS Flow GBR configuration settings 469

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	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size for IxStack	Set the custom value of the capture size for IxStack.
Enable Capture Circular Buffer for IxStack	Select this option to enable circular buffer capture for IxStack.
Enable Capture On Loopback Interface	Select this option to enable packet capture on the loopback interface.
Enable 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 <i>Automated Polling Interval</i> option is disabled. 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 enabled, 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	461
DNN GBR configuration settings	463
Session AMBR configuration settings	463

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	Enable this option if the UE subscription data indicates support for interworking with EPS for this DNN.
Is Local Area DN	<p>Enable 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	Enable this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.
Subscriber Spending Limits	Enable this option if the DNN will support PDU session policies that are based on subscriber spending limits.
Offline	Enable this option if the DNN will support the offline charging method for PDUs sessions.
Online	Enable this option if the DNN will support the online charging method for PDUs sessions.
GBR	Select this option to open a new panel that contains the GBR settings. These settings are described in DNN GBR configuration settings .
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 .

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

The following tables describes the Session AMBR configuration settings.

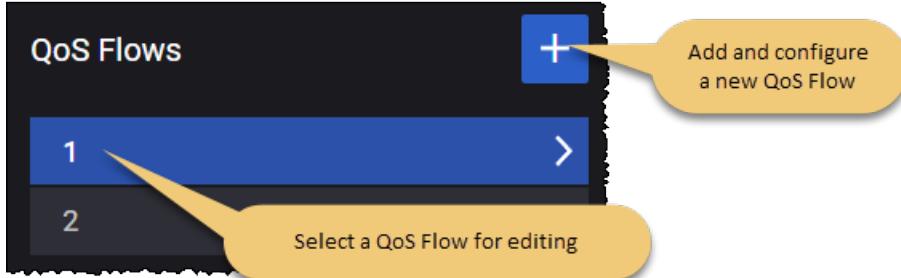
Parameter	Description
Session AMBR Uplink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Session AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Session AMBR Downlink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) downlink 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	465
QoS Flow Packet Filter configuration settings	467
QoS Flow Maximum Packet Loss configuration settings	468
QoS Flow ARP configuration settings	468
QoS Flow MBR configuration settings	469
QoS Flow GBR configuration settings	469

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.

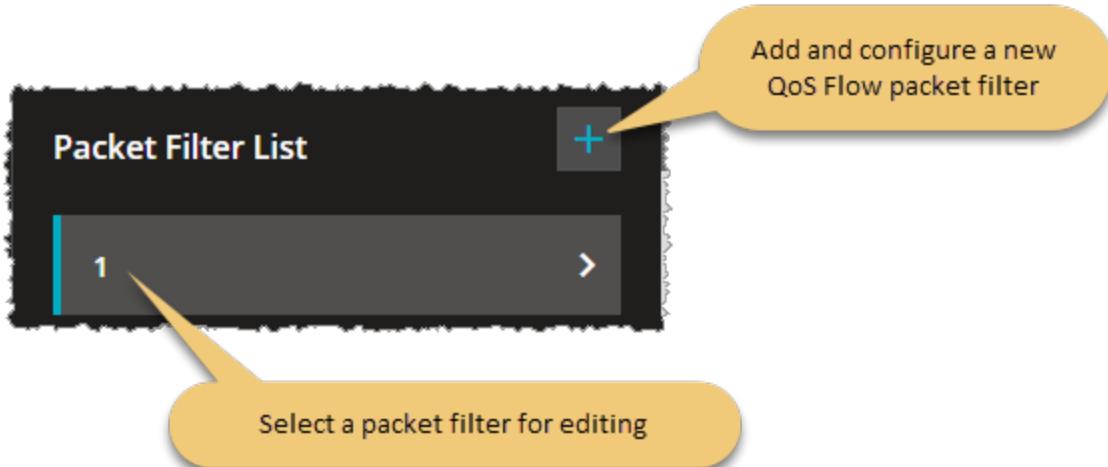
Setting	Description
<i>QoS Flow:</i>	
Is Default	<p>Enable this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow.</p> <p>If this option is not selected, LoadCore makes the Packet Filter List settings available for configuration (refer to QoS Flow Packet Filter configuration settings for descriptions of these settings).</p>
QFI	<p>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.</p>
5QI	<p>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.</p>
5QI Priority Level	<p>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.</p>
Resource Type	<p>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.</p>
Averaging Window	<p>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.</p>

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.</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.</p>
ARP	<p>Refer to the following topic for a description of the ARP configuration settings: QoS Flow ARP configuration settings.</p>
MBR	<p>Refer to the following topic for a description of the MBR configuration settings: QoS Flow MBR configuration settings.</p>
GBR	<p>Refer to the following topic for a description of the GBR configuration settings: QoS Flow GBR configuration settings.</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	Enable this option if the packets in this QoS Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.
Preemption Vulnerability	Enable this option if the packets in this QoS Flow are candidates for being preempted by other flows. When a flow is preemption-vulnerable, it can be dropped to free up resources for packets that have a higher ARP priority level.

QoS Flow MBR configuration settings

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

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

Setting	Description
<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.

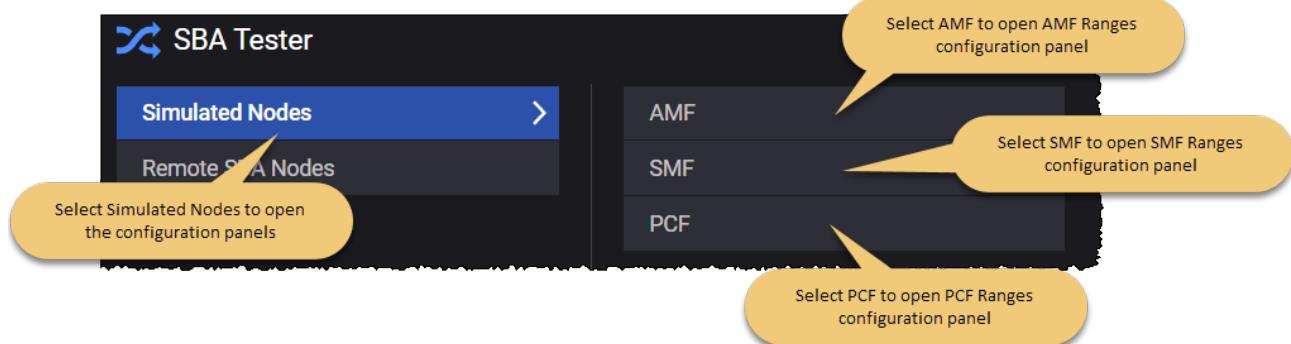
Setting	Description
<i>5G QoS Flow, GBR:</i>	
Uplink Bitrate Unit	Select the uplink bitrate unit from the drop-down list.
Uplink Bitrate Value	Set the guaranteed bit rate value for uplink traffic.
Downlink Bitrate Unit	Select the downlink bitrate unit from the drop-down list.
Downlink Bitrate Value	Set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



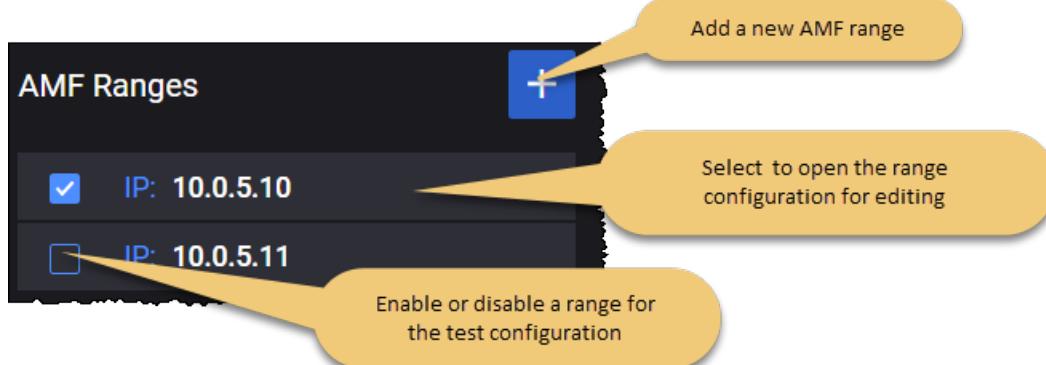
AMF configuration settings

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 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 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>

Setting	Description
Set ID	<p>An AMF Set consists of some AMFs that serve a given area and Network Slice. Multiple AMF Sets may be defined per AMF Region and Network Slice(s).</p> <p>The AMF Set ID to use for this simulated AMF node. The Set ID uniquely identifies the AMF Set within the AMF Region.</p>
Pointer	The AMF Pointer 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.
Indirect Communication without Delegated Discovery	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes	This option is available only if <i>Indirect Communication without Delegated Discovery</i> option is enabled. It allows the user to select the target nodes (UDM, AUSF, PCF, NSSF) for Indirect Communication via SCP.
Indirect Communication with Delegated Discovery	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes for Delegated Discovery	This option is available only if <i>Indirect Communication with Delegated Discovery</i> option is enabled. Select the targeted nodes from the drop-down list.
Optional Discovery Parameters	<p>A list of optional parameters for certain targets that can be used in discovery requests when using Delegated Discovery.</p> <p>This option is available only if <i>Indirect Communication with Delegated Discovery</i> option is enabled. For more details, refer to Optional Discovery Parameters.</p>

The following table describes the optional parameters required for delegated discovery.

Setting	Description
<i>Targeted Nodes</i>	
+	Select this button to add the a target node to your test configuration.

Setting	Description
<i>Settings</i>	
Target Node	
	Select the Delete Target Node button to remove this node from your test configuration.
Target Type	Select the target node from the drop-down list.
Discovery Parameter List	
Service Names	Select the service name from the drop-down list.
DNN	Select one of the configured DNNs from the drop-down list.
Hnrf Uri	Set the Uri value for this field.
supi	Set the subscription permanent identifier value.
gspi	Set the value for this field.
Routing Indicator	Provide the routing indicator value.
External Group Identity	Provide the external group identity value.
Dataset Id	Select an option from the drop-down list: <ul style="list-style-type: none"> • SUBSCRIPTION • POLICY • EXPOSURE • APPLICATION
Amf Region Id	Set the value for this field.
Network Instance Format	Select the encoding format for the network instance: string or label-list.
Target Nf Fqdn	Set the value for this field.
Pgw	Set the value for this field.
Amf Set Id	Set the value for this field.
Smf Serving Area	Set the value for this field.
UE IPv4 Address	Set the UE IPV4 address.
UE Ipv6 Prefix	Set the UE IPV6 address prefix.

Setting	Description
<i>SNssai</i>	
SST	Provide the SST (Slice/Service Type) value.
SD	Provide the SD (Slice Differentiator) value.
Mapped SST	Provide the mapped SST (Slice/Service Type) value.
Mapped SD	Provide the mapped SD (Slice Differentiator) value.
<i>Target Plmn List</i>	
	Select this button to add the a target plmn list to your test configuration.
	Select the Delete Target Plmn button to remove this list from your test configuration.
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
<i>Guami</i>	
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
Amf Id	Set the value for this field.
<i>TAI</i>	
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
TAC	Provide the Tracking Area Code (TAC) value.
<i>Nsi List</i>	
	Select this button to add the a Nsi list to your test configuration.
	Select this button to remove the Nsi list to your test configuration.

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
<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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<i>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.
<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.

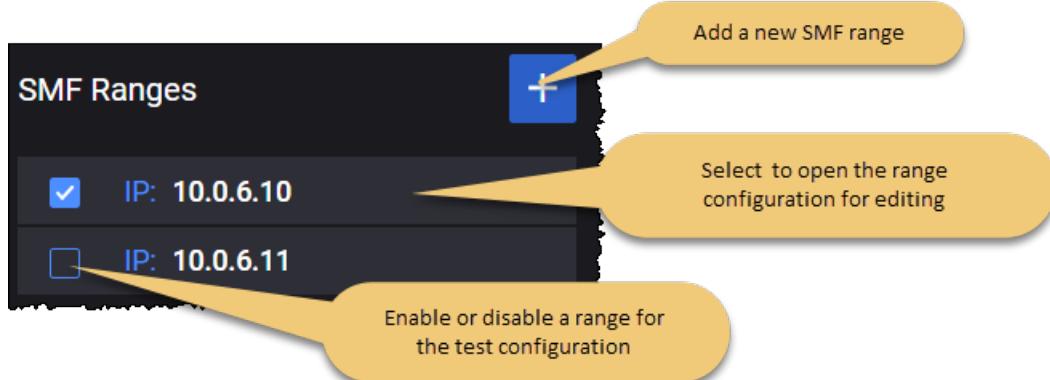
SMF configuration settings

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 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</p>

Setting	Description
	operator in that country, usually represented in the form 001-01 or 001-001. The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.
PLMN MNC	The PLMN MNC for this AMF range. About PLMN MNC ... The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.
Indirect Communication without Delegated Discovery	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes	This option is available only if <i>Indirect Communication without Delegated Discovery</i> option is enabled. It allows the user to select the target nodes (CHF, PCF) for Indirect Communication via SCP.
Indirect Communication with Delegated Discovery	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes for Delegated Discovery	This option is available only if <i>Indirect Communication with Delegated Discovery</i> option is enabled. Select the targeted nodes from the drop-down list.
Optional Discovery Parameters	A list of optional parameters for certain targets that can be used in discovery requests when using Delegated Discovery. This option is available only if <i>Indirect Communication with Delegated Discovery</i> option is enabled. For more details, refer to Optional Discovery Parameters .
SMF NSSAI:	
	Select the Add NSSAI button to add a NSSAI to your test configuration.
SMF NSSAI:	
	Select the Delete NSSAI button to remove this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.

Setting	Description
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.

The following table describes the optional parameters required for delegated discovery.

Setting	Description
<i>Targeted Nodes</i>	
	Select this button to add the a target node to your test configuration.
<i>Settings</i>	
Target Node	
	Select the Delete Target Node button to remove this node from your test configuration.
Target Type	Select the target node from the drop-down list.
<i>Discovery Parameter List</i>	
Service Names	Select the service name from the drop-down list.
DNN	Select one of the configured DNNs from the drop-down list.
Hnrf Uri	Set the Uri value for this field.
supi	Set the subscription permanent identifier value.
gspi	Set the value for this field.
Routing Indicator	Provide the routing indicator value.
External Group Identity	Provide the external group identity value.
Dataset Id	Select an option from the drop-down list: <ul style="list-style-type: none"> • SUBSCRIPTION • POLICY • EXPOSURE • APPLICATION

Setting	Description
Amf Region Id	Set the value for this field.
Network Instance Format	Select the encoding format for the network instance: string or label-list.
Target Nf Fqdn	Set the value for this field.
Pgw	Set the value for this field.
Amf Set Id	Set the value for this field.
Smf Serving Area	Set the value for this field.
UE IPv4 Address	Set the UE IPV4 address.
UE Ipv6 Prefix	Set the UE IPV6 address prefix.
<i>SNssai</i>	
SST	Provide the SST (Slice/Service Type) value.
SD	Provide the SD (Slice Differentiator) value.
Mapped SST	Provide the mapped SST (Slice/Service Type) value.
Mapped SD	Provide the mapped SD (Slice Differentiator) value.
<i>Target Plmn List</i>	
	Select this button to add the a target plmn list to your test configuration.
	Select the Delete Target Plmn button to remove this list from your test configuration.
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
<i>Guami</i>	
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
Amf Id	Set the value for this field.
<i>TAI</i>	
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.

Setting	Description
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
TAC	Provide the Tracking Area Code (TAC) value.
Nsi List	
	Select this button to add the a Nsi list to your test configuration.
	Select this button to remove the Nsi list to your test configuration.

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
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).
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.

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.
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.

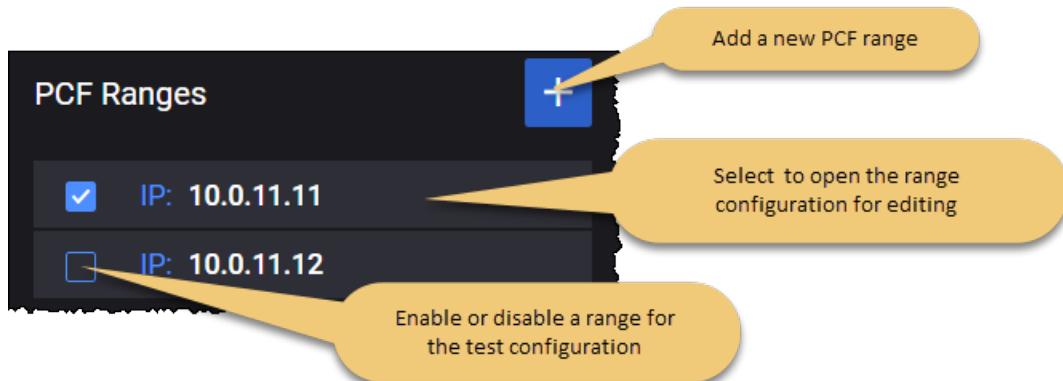
PCF configuration settings

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
PCF:	

Setting	Description
	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 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	<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>
Indirect Communication without Delegated Discovery	This option is available only if SCP is selected in SCP Connection Settings .
Target Nodes	This option is available only if <i>Indirect Communication without Delegated Discovery</i> option is enabled. It allows the user to select the target node (CHF) for Indirect Communication via SCP.
Indirect Communication with Delegated Discovery	This option is available only if SCP is selected in SCP Connection Settings .

Setting	Description
Target Nodes for Delegated Discovery	This option is available only if <i>Indirect Communication with Delegated Discovery</i> option is enabled. Select the targeted nodes from the drop-down list.
Optional Discovery Parameters	A list of optional parameters for certain targets that can be used in discovery requests when using Delegated Discovery. This option is available only if <i>Indirect Communication with Delegated Discovery</i> option is enabled. For more details, refer to Optional Discovery Parameters .

The following table describes the optional parameters required for delegated discovery.

Setting	Description
<i>Targeted Nodes</i>	
	Select this button to add the a target node to your test configuration.
<i>Settings</i>	
<i>Target Node</i>	
	Select the Delete Target Node button to remove this node from your test configuration.
<i>Target Type</i>	Select the target node from the drop-down list.
<i>Discovery Parameter List</i>	
<i>Service Names</i>	Select the service name from the drop-down list.
<i>DNN</i>	Select one of the configured DNNs from the drop-down list.
<i>Hnrf Uri</i>	Set the Uri value for this field.
<i>supi</i>	Set the subscription permanent identifier value.
<i>gspi</i>	Set the value for this field.
<i>Routing Indicator</i>	Provide the routing indicator value.
<i>External Group Identity</i>	Provide the external group identity value.
<i>Dataset Id</i>	Select an option from the drop-down list: <ul style="list-style-type: none"> • SUBSCRIPTION • POLICY

Setting	Description
	<ul style="list-style-type: none"> • EXPOSURE • APPLICATION
Amf Region Id	Set the value for this field.
Network Instance Format	Select the encoding format for the network instance: string or label-list.
Target Nf Fqdn	Set the value for this field.
Pgw	Set the value for this field.
Amf Set Id	Set the value for this field.
Smf Serving Area	Set the value for this field.
UE IPv4 Address	Set the UE IPV4 address.
UE Ipv6 Prefix	Set the UE IPV6 address prefix.
<i>SNssai</i>	
SST	Provide the SST (Slice/Service Type) value.
SD	Provide the SD (Slice Differentiator) value.
Mapped SST	Provide the mapped SST (Slice/Service Type) value.
Mapped SD	Provide the mapped SD (Slice Differentiator) value.
<i>Target Plmn List</i>	
	Select this button to add the a target plmn list to your test configuration.
	Select the Delete Target Plmn button to remove this list from your test configuration.
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
<i>Guami</i>	
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
Amf Id	Set the value for this field.
<i>TAI</i>	

Setting	Description
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.
PLMN MNC	Provide the PLMN MNC (Mobile Network Code) value.
TAC	Provide the Tracking Area Code (TAC) value.
<i>Nsi List</i>	
	Select this button to add the a Nsi list to your test configuration.
	Select this button to remove the Nsi list to your test configuration.

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.

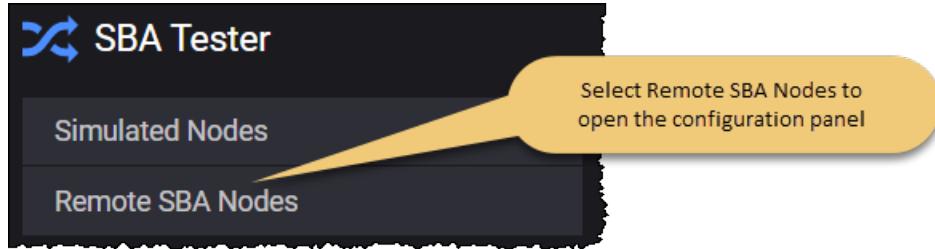
NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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.
TCP Connections	The number of concurrent TCP connections to use for each DUT.
<i>Additional Routes</i>	The additional routes will use the gateway defined in the IP information below.
	Select this button to add a new additional route to your test configuration, if needed.

Connectivity Settings	Description
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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.

Discovery Settings

This section is available only when the **Peer NRF** is set to an IP address.

Setting	Description
Select Node Type for Discovery	<p>This option allows the user to select which node should be discovered by the SBA Tester.</p> <p>Select the node (or nodes) from the drop-down list.</p> <p>Available options: AUSF, CHF, NSSF, PCF and UDM.</p>

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.

Setting	Description
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.

AUSF configuration settings	491
AUSF Ranges panel	492
AUSF Range panel	492
AUSF node settings	493
AUSF Nauf interface settings	494
AUSF remote SBA nodes	495
CHF configuration settings	497
CHF Ranges panel	497
CHF Range panel	498
CHF node settings	498
CHF Nchf interface settings	499
CHF remote SBA nodes	500
NRF configuration settings	500
NRF Ranges panel	501
NRF Range panel	501
NRF node settings	502
NRF Nnrf interface settings	503
NSSF configuration settings	505
NSSF Ranges panel	506
NSSF Range panel	506
NSSF node settings	507
Nnssf Interface Settings	508
Remote SBA nodes	509
NSSF Restricted NSSAIs	510
NSSF Network Slices	511
NSSF Configured NSSAI	512
PCF configuration settings	513
PCF Ranges panel	513
PCF Range panel	513

PCF node settings	514
PCF service area restrictions	516
PCF Npcf interface settings	517
PCF remote SBA nodes	518
SCP configuration settings	519
SCP Ranges panel	519
SCP Range panel	520
SCP Nscp interface settings	521
SCP Remote SBA Nodes	522
UDM configuration settings	523
UDM Ranges panel	523
UDM Range panel	524
UDM node settings	524
UDM Nudm interface settings	527
UDM remote SBA nodes	529
UDR configuration settings	529
UDR Ranges panel	530
UDR Range panel	530
UDR Nudr interface settings	531
UDR remote SBA nodes	532

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	492
AUSF Range panel	492
AUSF node settings	493
AUSF Nausf interface settings	494
AUSF remote SBA nodes	495

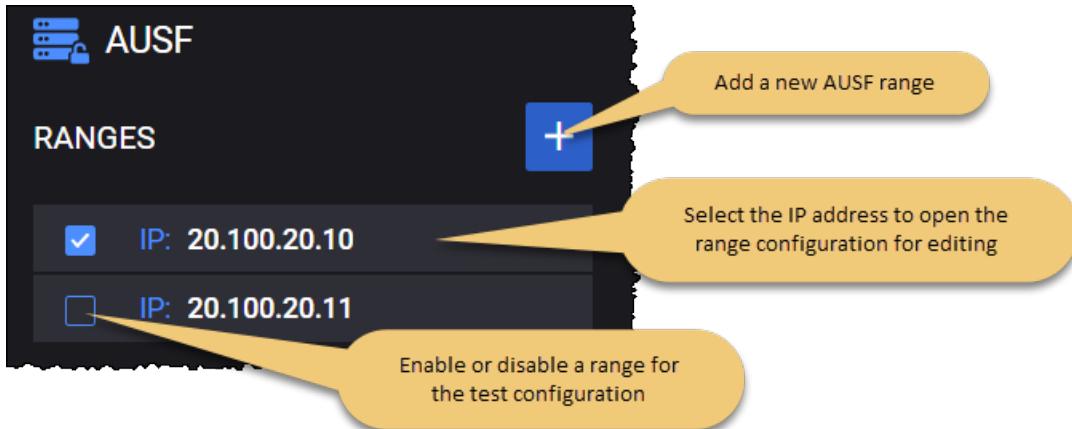
AUSF Ranges panel

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 it is selected in the Topology window).

Setting	Description
<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 .
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 .
Remote SBA Nodes	These settings are described in AUSF remote SBA nodes .

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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if

Connectivity Settings	Description
	needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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 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.
Indirect Communication without Delegated	<p>IMPORTANT <i>This option is visible only when SCP is selected in SCP Connection Settings.</i></p>

Setting	Description
Discovery	Select the option to enable it. For more details, refer to Indirect Communication without Delegated Discovery .

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:

- **Indirect Communication without Delegated Discovery**

If Indirect Communication with or without Delegated Discovery option is enabled for one or more nodes from Remote SBA Nodes, then only the messages for the interface on which this option is enabled will be forwarded to the SCP. In the case of Indirect Communication with Delegated Discovery, SCP will also perform delegated discovery.

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 (to set the PCF as a DUT refer to [PCF range controls and settings](#)).

The configuration settings are described in the topics listed below.

CHF Ranges panel	497
CHF Range panel	498
CHF node settings	498
CHF Nchf interface settings	499
CHF remote SBA nodes	500

Topics:

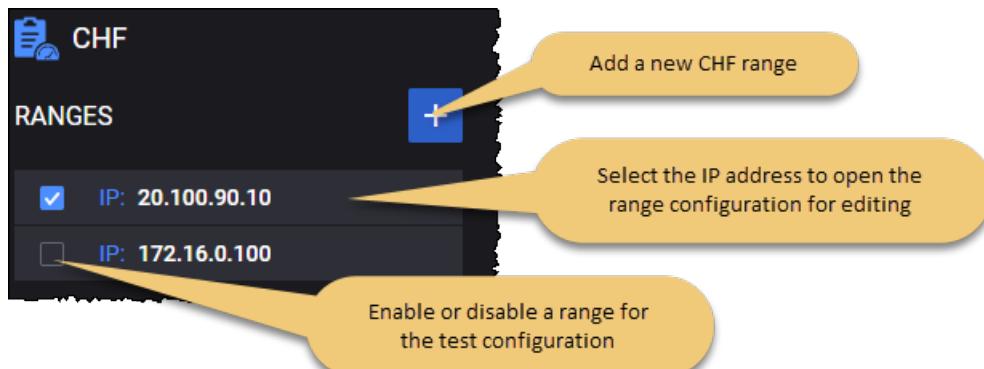
CHF Ranges panel

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 the configuration of an associated set of Node Settings, which are described in CHF node settings .
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 .
Remote SBA Nodes	These settings are described in CHF remote SBA nodes .

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
<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.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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>

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.

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 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.

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	501
NRF Range panel	501
NRF node settings	502
NRF Nnrf interface settings	503

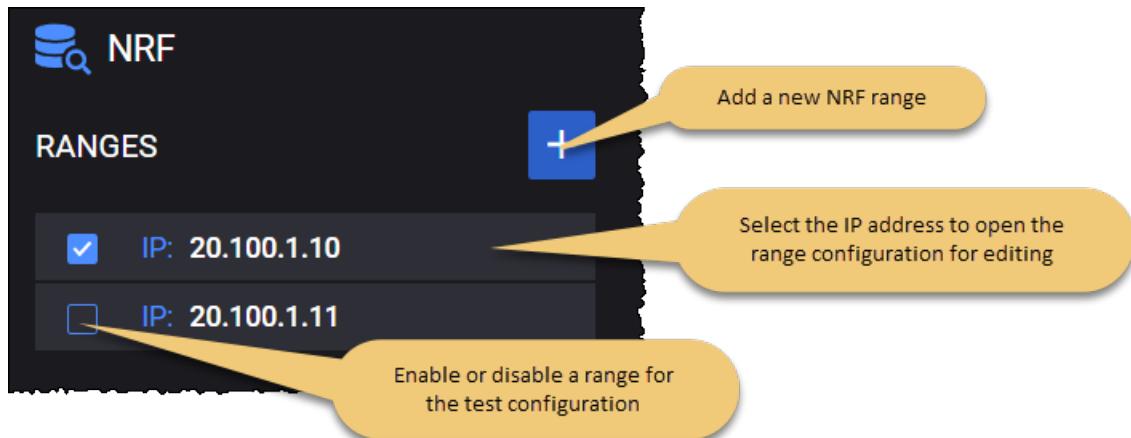
NRF Ranges panel

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 .
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 .

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 ... The Mobile Network Code (MNC) is a two-digit (North America) or three-digit

Setting	Description
	(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.

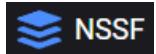
The following **Connectivity Settings** enable the necessary Nnrf connectivity and service interaction.

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
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.

Connectivity Settings	Description
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

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	506
NSSF Range panel	506
NSSF node settings	507
Nnssf Interface Settings	508
Remote SBA nodes	509
NSSF Restricted NSSAIs	510
NSSF Network Slices	511
NSSF Configured NSSAI	512

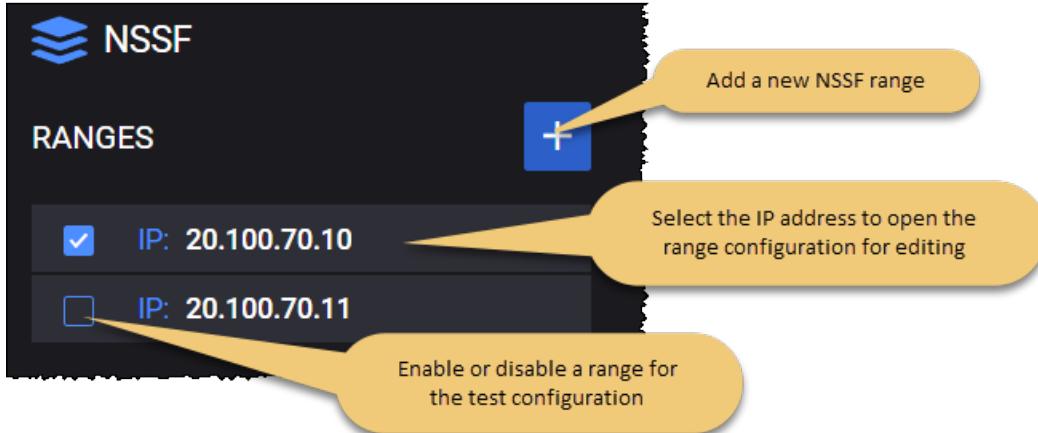
NSSF Ranges panel

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.
Device Under Test	Enable this option if your NSSF is a DUT in this test configuration.

Setting	Description
	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 .
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 .
Remote SBA Nodes	These settings are described in Remote SBA nodes .
<i>Network Slicing:</i>	
Restricted NSSAIs	These settings are described in NSSF Restricted NSSAIs .
Network Slices	These settings are described in NSSF Network Slices .
Configured NSSAIs	These settings are described in NSSF Configured NSSAI .

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	<p>Multiple NSSF instances may be deployed in the 5G network.</p> <p>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.</p>
PLMN 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>

Setting	Description
	The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.
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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.

Connectivity Setting	Description
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<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>	
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

Setting	Description
	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 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

Setting	Description
	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.

Setting	Description
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 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	513
PCF Range panel	513
PCF node settings	514
PCF service area restrictions	516
PCF Npcf interface settings	517
PCF remote SBA nodes	518

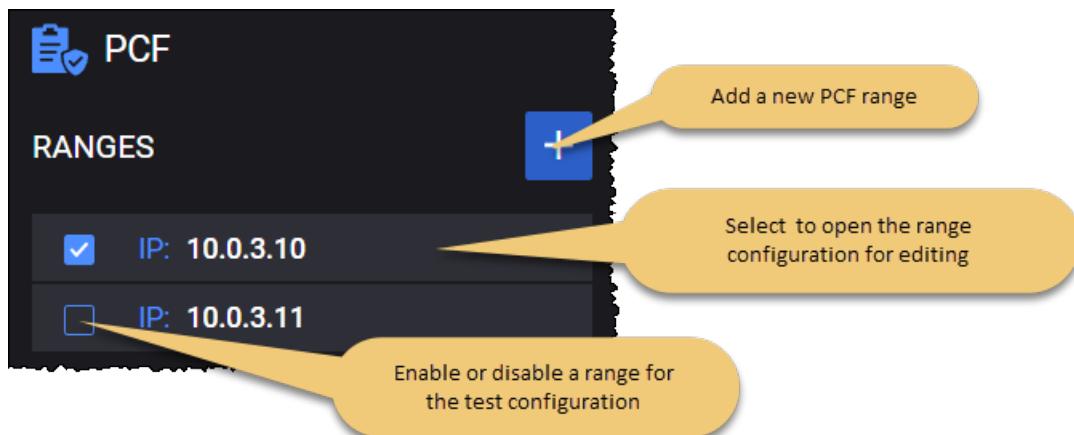
PCF Ranges panel

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 .
Service Area Restrictions	Each PCF range requires the configuration of the service area restrictions. The settings are described in PCF service area restrictions .
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 .
Remote SBA Nodes	These settings are described in PCF remote SBA nodes .

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	Multiple PCF instances may be deployed in the 5G network. 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.
MCC	The PLMN MCC for this PCF range.

Setting	Description
	<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.
Include Request in Response	Enable this option to include the request in the response message.
Default Charging Method Offline	If needed, enable this option.
Default Charging Method Online	If needed, enable this option.
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. • Service Area Restriction Change • RFSP CHRA Change • Manage UE Policy Message <p>Multiple values can be selected simultaneously.</p>

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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.

Connectivity Settings	Description
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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

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	The IP address from your test network to use for Nudr traffic. This 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.

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 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:

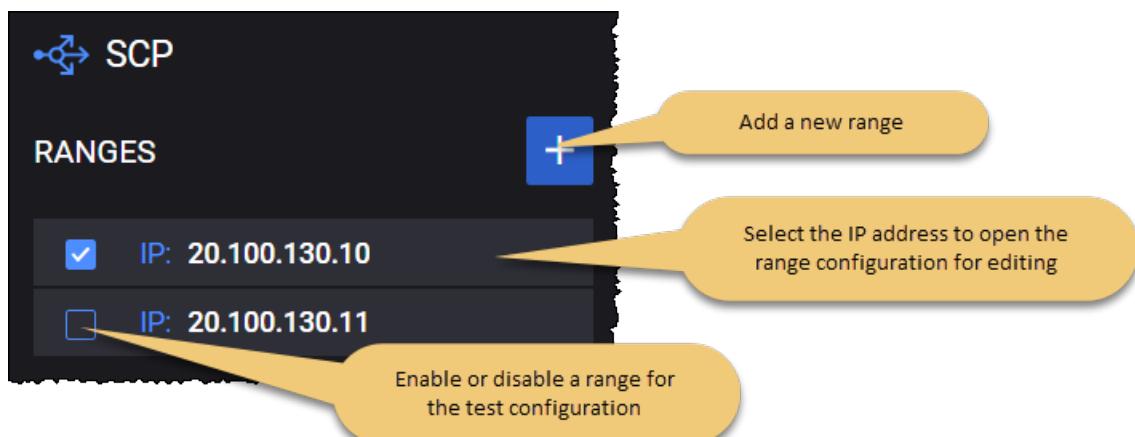
SCP Ranges panel	519
SCP Range panel	520
SCP Nscp interface settings	521
SCP Remote SBA Nodes	522

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	Each SCP range requires the configuration of an associated set of Node Settings, which are described in SCP node settings .
Nscp 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 Nscp interface settings .
Remote SBA Nodes	The remote SBA node settings are described in SCP remote SBA nodes .

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.
Enable	Select this option to enable delegated discovery.

Setting	Description
Delegated Discovery	
HTTP Connections	The number of HTTP connections between two nodes.

SCP Nscp 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.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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>

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.

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.

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.

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	523
UDM Range panel	524
UDM node settings	524
UDM Nudm interface settings	527
UDM remote SBA nodes	529

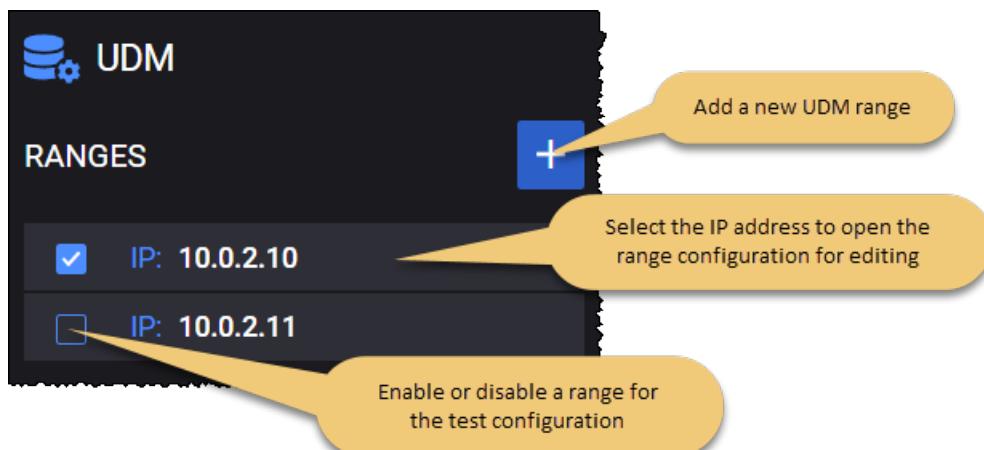
UDM Ranges panel

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 the configuration of an associated set of Node Settings, which are described in UDM node settings .
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 Nudm interface settings .
Remote SBA Nodes	These settings are described in UDM remote SBA nodes .

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	The PLMN MCC for this UDM range.

Setting	Description
	<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> <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>

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.

Setting	Description
	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 remote 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.

Setting	Description
<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="border: 1px solid #0056b3; padding: 2px; margin-left: 20px;"> IMPORTANT This field must have a valid JSON text value only if the Change type is set to Add or Replace. </div>
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)	<div style="background-color: #e0e0e0; padding: 2px; margin-right: 10px;"> NOTE </div> 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.

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.

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

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.

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	530
-------------------------	------------

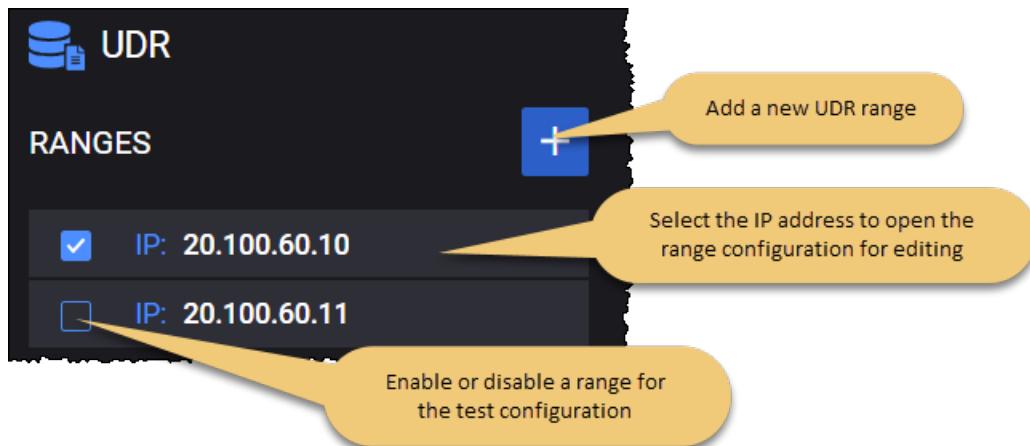
UDR Range panel	530
UDR Nudr interface settings	531
UDR remote SBA nodes	532

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.

Setting	Description
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. 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 .
Remote SBA Nodes	These settings are described in UDR remote SBA nodes .

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
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.
Additional	<i>The additional routes will use the gateway defined in the IP information below.</i>

Connectivity Settings	Description
Routes	
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
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.

UDR remote SBA nodes

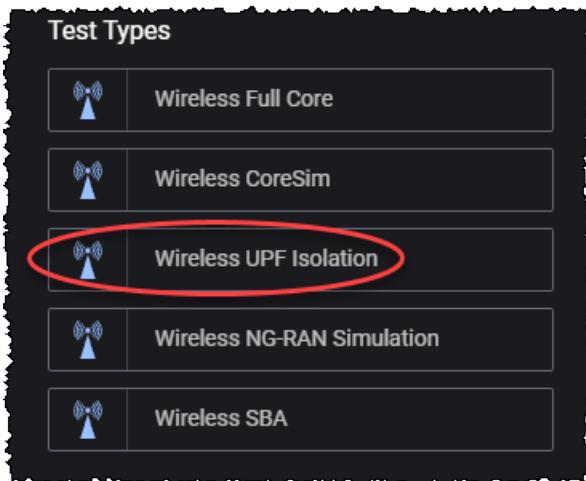
To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

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.

CHAPTER 10

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	536
DNS Settings	537
Advanced Settings	537
Impairment	539
QoS Flows panel	540
QoS Flow configuration settings	540
Reporting Settings	542
UE configuration settings	543
UE Ranges panel	544
UE Range panel	545
UE range settings	546

Objectives	551
Control Plane Objective	551
About primary objectives	552
Primary Control Plane Objective	554
Secondary Control Plane Objectives	556
User Plane Objectives	564
Stateless UDP Traffic Generator	566
Data Traffic	567
Voice Traffic	571
Video OTT Traffic	585
DNS Client Traffic	589
ICMP Client	592
Predefined Applications Traffic	593
Capture Replay	603
DN configuration settings	606
DN Ranges panel	606
DN Range panel	607
DN N6 Interface settings	608
DN routes settings	609
DN User Plane	609
DN Stateless UDP Traffic	610
DN Data Traffic	611
DN Voice Traffic	614
DN Video OTT Traffic	626
DN DNS Server Traffic	628
DN Predefined Applications Traffic	631
DN Capture Replay	631
RAN configuration settings	634
RAN Ranges panel	635
RAN Range settings	635
RAN N3 interface settings	636
Passthrough interface settings	637

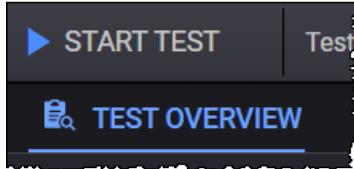
SMF configuration settings	638
SMF Ranges panel	639
SMF Range settings	639
SMF N4 interface settings	640
SMF Uplink Paths	642
UPF configuration settings	644
UPF Ranges panel	645
UPF Range panel	645
UPF N3 interface settings	646
UPF N4 interface settings	647
UPF N6 interface settings	649
UPF N9 interface settings	650
UPF N4u interface settings	651

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:

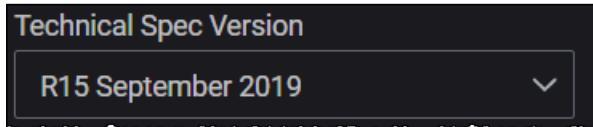


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



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 **537**

Advanced Settings **537**

Impairment **539**

QoS Flows panel **540**

 QoS Flow configuration settings 540

 Reporting Settings 542

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	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size for IxStack	Set the custom value of the capture size for IxStack.
Enable Capture Circular Buffer for IxStack	Select this option to enable circular buffer capture for IxStack.
Enable Capture On Loopback Interface	Select this option to enable packet capture on the loopback interface.
Enable Control Plane Advanced Stats	By default, these measurements and statistics are disabled. Select this option to enable control plane latency statistics.
Enable User	Select an option from the drill-down list for the user plane advanced statistics:

Setting	Description
Plane Advanced Stats	<ul style="list-style-type: none"> • None - no advanced statistics enabled. • One Way Delay - the time spent by the packet on the network from the moment it is sent until it is received. • Delay Variation Jitter - the per polling interval average delay variation jitter value calculated for all packets.
Automated Polling Interval	Enabled 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 option is disabled.</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	When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.

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	Set the count value.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable RTP.

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

Impairment

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

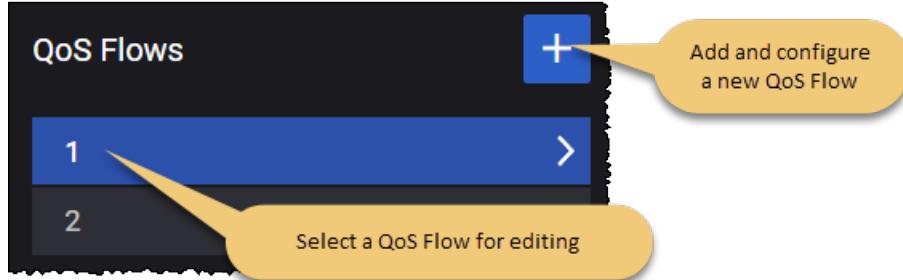
Setting	Description
<i>Impairment Profiles:</i>	
	Select the Add impairment profile button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the Delete impairment profile button to remove the profile from your test configuration.
Name	Each impairment profile is uniquely 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 **540**

Reporting Settings **542**

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	Enable this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow. 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 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.

Setting	Description
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 \$ueip\$ (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.

Active Predefined Rules:

	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:

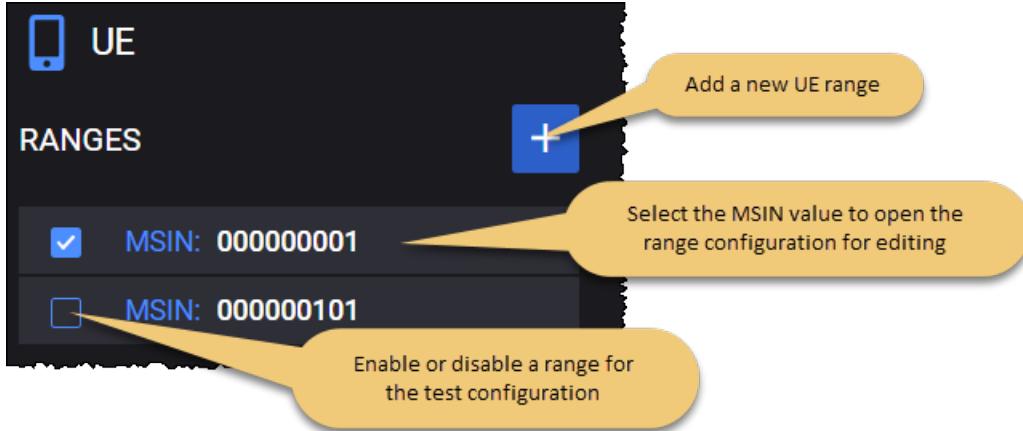
UE Ranges panel	544
UE Range panel	545
UE range settings	546

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](#) 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 .
Settings	Refer to the following topic for descriptions of the UE Settings settings: Settings .
QoS Config	Refer to the following topic for descriptions of the UE QoS Config settings: QoS Config settings .

Objectives

Each UE range has its own objectives settings. Refer to [Objectives](#) 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, 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	Enable this option 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	Enable this option 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	Enable this option to include the IMEI SV in the UserID IE.
IMEI	<p>The IMEI value that will be assigned to the first simulated UE in the range.</p> <p>The International Mobile Equipment Identity (IMEI) is a number used to uniquely identify 3GPP and iDEN mobile phones, as well as some satellite phones. It identifies the origin, model, and serial number of the device. It consists of either 15 digits (14 digits plus one check digit); or 16 digits (14 digits plus two software version digits). GSM networks use the IMEI number to identify valid devices, and can also use the number to prevent a stolen phone from accessing the network.</p> <p>When it includes the software version digits, it is referred to as the IMEISV.</p>
IMEI Increment	The value to use for incrementing the IMEI values for each of the UEs in the range.
Software Version	The software version number identifies the software version number of the mobile equipment. Its length is 2 digits.

Settings

The following table describes the UE 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	When this option 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	<p>This option enables IPv6 UEs to get their IP addresses via SLAAC (Stateless Address Auto-configuration).</p> <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.
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>

Setting	Description
	<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 [start_value-end_value,increment].</p> <p>NOTE The start_value and end_value must have the same length. For example, we can configure dnn[008-999,1] and obtain dnn008,dnn009,...,dnn998,dnn999. Syntaxes dnn[8-999,1] or [008-1000,1] are not valid as the start and end value lengths are different.</p> <p>The start value is mandatory. Omitting certain parameters results in behaviors as exemplified below:</p> <ul style="list-style-type: none"> • dnn[4-9,] an implicit increment of 1 is used • dnn[4-9] as above • dnn[4-,1] is used as dnn[4-9,1], 9 being the maximum value with the configured length, length of 1 in this case • dnn[4-,] as above • dnn[4-] as above • dnn[4] as above <p>UEs will use the DNN values from the pool in a round robin manner.</p> <p>IMPORTANT If multiple sequence generators are configured and their pools overlap (for example: dnn[000-600,1].keysight.com dnn[500-999,1].keysight.com), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the start_value (they might start with an intermediate value in the second pool).</p>

BAR Settings: These settings are used in the Update BAR procedure for idle UEs.

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).
Suggested Buffering Packets Count	The count of suggested buffering packets.
<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 this option 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 this option 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.

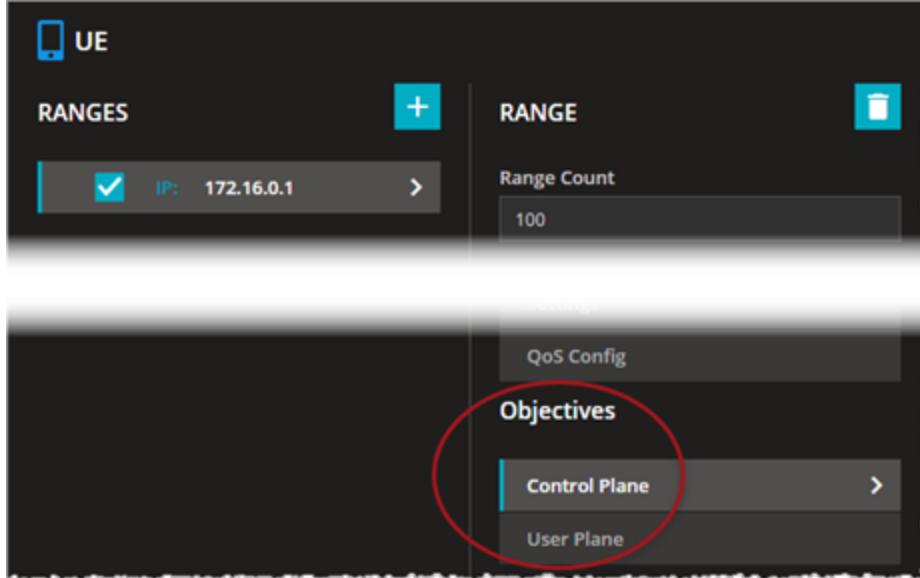
Objectives

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](#)
- [User Plane Objectives](#)

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

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

Active Subscribers

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

<i>Ramp Up Time:</i>	20000 / 1000 = 20s for subscribers to register
<i>Rate in ramp up time:</i>	1000 registrations per second

<i>Sustain time:</i>	30 seconds
<i>Rate in sustain time:</i>	2000 secondary procedures per second
<i>Ramp down time:</i>	$20000 / 1000 = 20$ 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

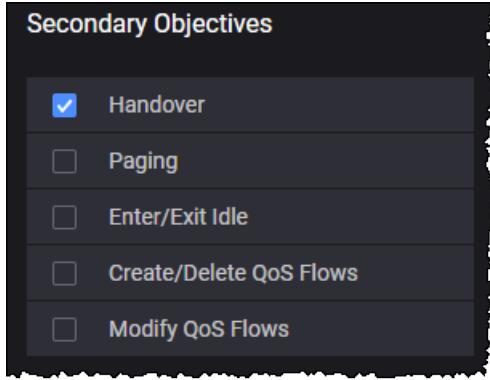
The following table describes the **Primary** control plane objectives.

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 after NG-Setup/S1-Setup have successfully completed.
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 after NG-Setup/S1-Setup have successfully completed.
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](#)). 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>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which handovers are initiated, measured in handovers per second.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of 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.

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

Parameter	Description
	<p>the DN IP address.</p> <ul style="list-style-type: none"> 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 UE is scheduled to Exit Idle but the UE state is not Idle anymore (for example Paging event occurred), the Exit Idle procedure cannot be performed, therefore the Service Request is going to be skipped and the statistics for Service Request Skipped (on NG-RAN) will be incremented accordingly.

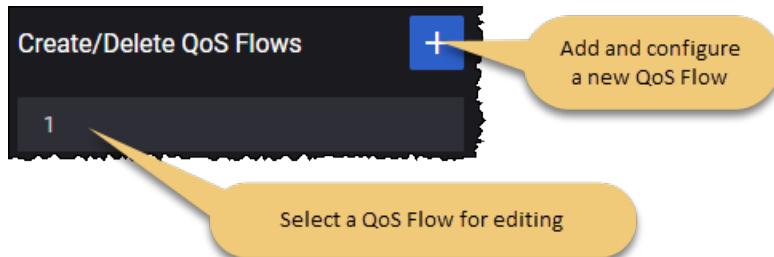
The following table describes the objective parameters.

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

Create/Delete QoS Flows:

When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to 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.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, once the sustain value is reached.
Interval	The number of seconds to wait between each successive action.
Flow IDs	Select the flow IDs from the drop-down list.

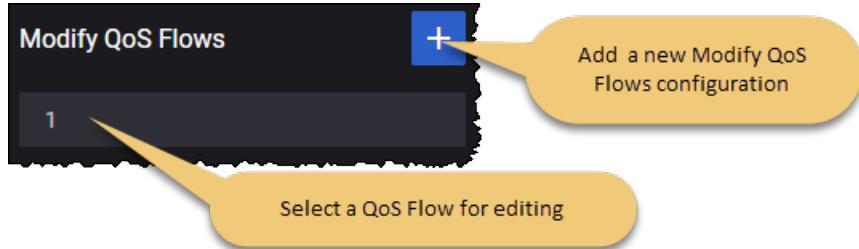
Modify QoS Flows

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.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds 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 below.
Update QoS	These settings are described in Update QoS below.

Parameter	Description
Update URR	These settings are described in Update URR 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.

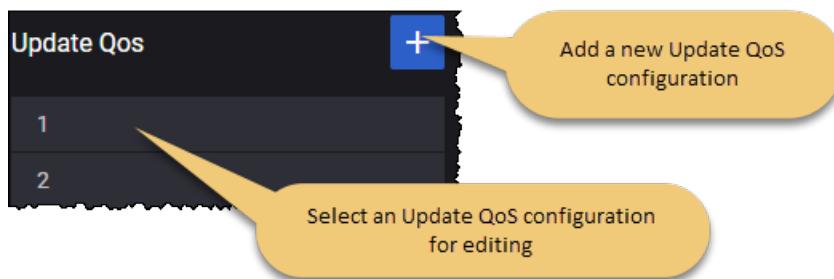


The following table describes the parameters required to update the packet detection rule.

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.
	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.



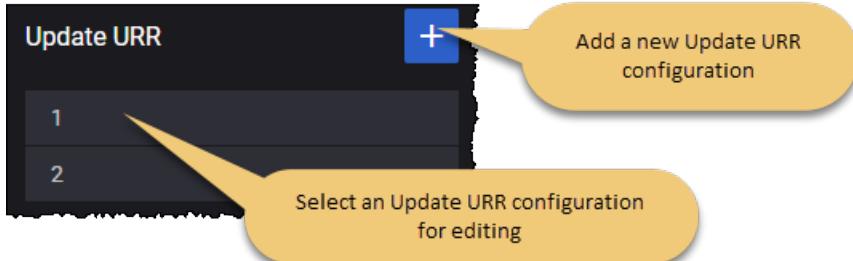
The following table describes the Update QoS settings.

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	<p>Select the desired Maximum Bit Rate (MBR) type for the flow. Based on your selection, LoadCore will present the appropriate settings.</p> <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> <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> <tr> <td>Downlink Action</td> <td>Select the action type to apply to the downlink bitrate.</td> </tr> <tr> <td>Downlink Step</td> <td>Select the step to increase or decrease the downlink bitrate.</td> </tr> </tbody> </table>	<i>QoS Rates:</i>		Parameter	Description	Uplink	Set the uplink bitrate.	Downlink	Set the downlink bitrate.	<i>Dynamic QoS Rates:</i>		Parameter	Description	Uplink Action	Select the action type to apply to the uplink bitrate.	Uplink Step	Select the step to increase or decrease the uplink bitrate.	Downlink Action	Select the action type to apply to the downlink bitrate.	Downlink Step	Select the step to increase or decrease the downlink bitrate.
<i>QoS Rates:</i>																					
Parameter	Description																				
Uplink	Set the uplink bitrate.																				
Downlink	Set the downlink bitrate.																				
<i>Dynamic QoS Rates:</i>																					
Parameter	Description																				
Uplink Action	Select the action type to apply to the uplink bitrate.																				
Uplink Step	Select the step to increase or decrease the uplink bitrate.																				
Downlink Action	Select the action type to apply to the downlink bitrate.																				
Downlink Step	Select the step to increase or decrease the downlink bitrate.																				
<i>Gate Status:</i>																					
Uplink	<p>Select an option from the drop-down list. Traffic is forwarded when the gate is open and discarded when the gate is closed.</p>																				
Downlink	Select an option from the drop-down list.																				

Parameter	Description
	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.



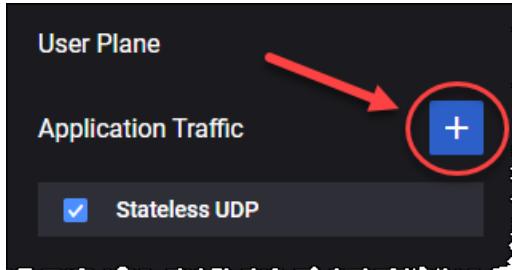
The following table describes the Update URR settings.

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**, **Predefined Applications**, **ICMP Client** and **Ping**.

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 .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Flow Type	This field is set to uplink and can not be modified since on the UE you can only configure the uplink flow.
Packet Rate	The rate at which the test generates packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
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

Parameter	Description
	<p>back to the default flow.</p> <ul style="list-style-type: none"> When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>

Data Traffic

The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Throughput . The other options are: Concurrent Connections and Connections Rate .
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to Concurrent Connections .
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to Concurrent Connections .
Connections Rate per Second	Set the value for connections rate per second. This parameter is available only when Objective type is set to Connections Rate .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single,

Parameter	Description
	unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
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 for a description of the configuration settings for these traffic flows. Also, you can add custom parameters, based on your test configuration requirements.</p>

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> If Optimize Throughput (per UE) option is enabled: TCP, TLS, QUIC or UDP. If Optimize Throughput (per UE) option is disabled: TCP, TLS or UDP.
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get, HTTP Put, HTTP Post and FTP. For TLS transport protocol: HTTPS Get, HTTPS Put and HTTPS Post. For QUIC transport protocol: HTTP3 Get, HTTP3 Put and HTTP3 Post. For UDP transport protocol: UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket) <p>NOTE UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receive the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds.</p>
Port	The port used by the flow.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
URL	The URL that is being accessed by the flow's protocol.

Parameter	Description
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.
Enable DNS Query Per Connection	Select the check-box to process only one DNS query per TCP connection.
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

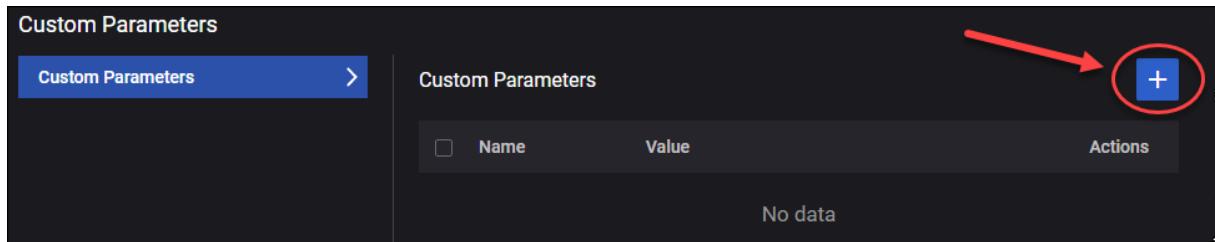
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

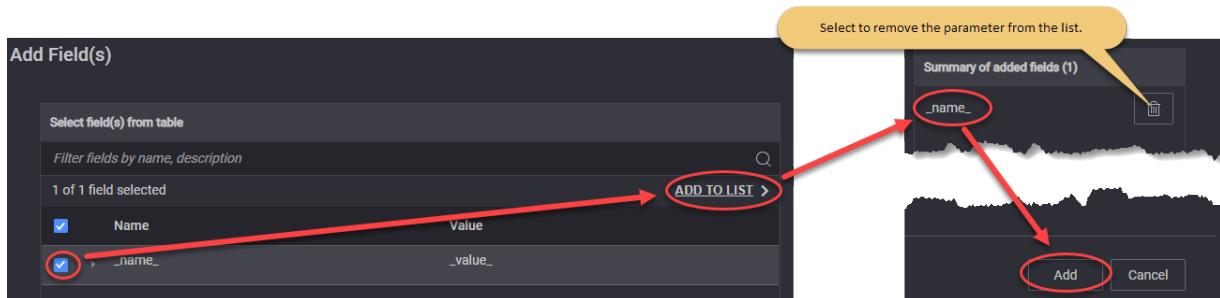
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Call Type	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 • UDP - User Datagram Protocol
Enable IPSEC	Select this option to enable IPSEC.
Domain	Provide the domain name.

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

Dial Plan

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

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

Parameter	Description
Destination Port	The destination port number.

Media Settings

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

Parameter	Description
Media Duration (ms)	Length of time to play the media stream. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID for Voice	The QoS Flow ID for RTP traffic. Select the QoS Flows ID(s) from the drop-down list.
Enable video	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for video from the drop-down list. This parameter is available only when Enable video is selected.

Jitter Buffer Settings:

Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
--------------------	--

Audio Codecs

	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: <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

Parameter	Description
	<ul style="list-style-type: none"> • G723 • G729 <p>The parameters of each audio codec are presented below.</p>
Video Codecs	<i>This section is available only when Enable video is selected</i>
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: H264 or H265 .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.
<i>Advanced Media Settings</i>	
Custom SDP	Select this panel to open the custom SDP settings.
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4 • NB Codecs IPv6 • AMR-WB IPv6 • Multimedia IPv4
QoE Settings	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

AMR/AMR-WB

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

Parameter	Description
Payload Type	Specifies the audio payload type.
Payload Format	<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.

Advanced SIP Settings

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

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

SIP Custom Headers

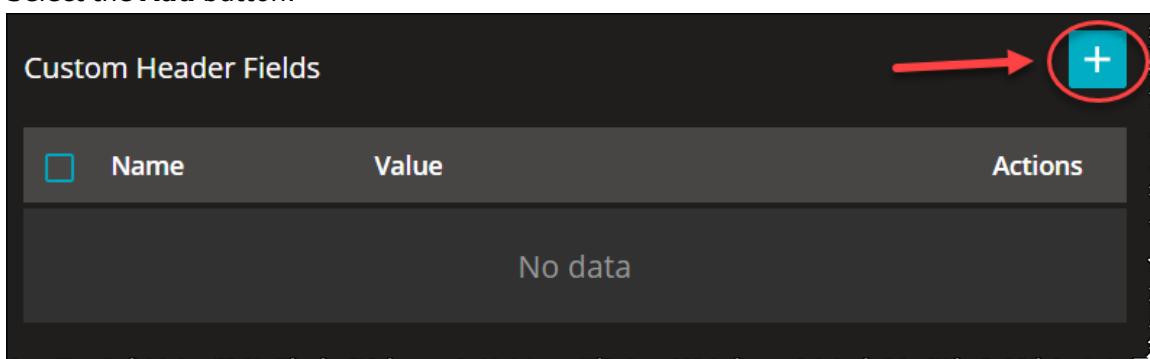
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE

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

For each message, you can:

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



The Add Field(s) opens.

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

For example ...

Add Field(s)

Select field(s) from table

Filter fields by name, description

1 of 63 fields selected

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	Accept	application/sdp,message/cpim
<input type="checkbox"/>	Accept-Contact	*;mobility="mobile";methods="INVITE"
<input checked="" type="checkbox"/>	Accept-Encoding	gzip
<input type="checkbox"/>	Accept-Language	da, en-gb;q=0.8, en;q=0.7
<input type="checkbox"/>	Alert-Info	<urn:alert:service:call-waiting>

Select to remove the field from the list.

Summary of added fields (1)

Accept-Encoding

The following custom header are available:

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

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

Parameter	Description	Value
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC 4028	60
Organization	IETF RFC 3261	Keysight
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC 3327	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>
P-Called-Party-ID	IETF RFC 7315	sip:user1-business@example.com
P-Charging-Function-Addresses	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Charging-Vector	IETF RFC 7315	icid-value=1234bc9876e;icid-generated-at=192.0.6.8;orig- ioi=home1.net

Parameter	Description	Value
P-Early-Media	IETF RFC 5009	supported
Permission-Missing	IETF RFC 5360	userC@example.com
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=False,algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-	IETF	<sip:server10.biloxi.com;lr>,

Parameter	Description	Value
Route	RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org?Replaces=425928%40bobster.example.com.3%3Bto-tag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF	12345

Parameter	Description	Value
	RFC 3903	
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

SIP Authentication

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

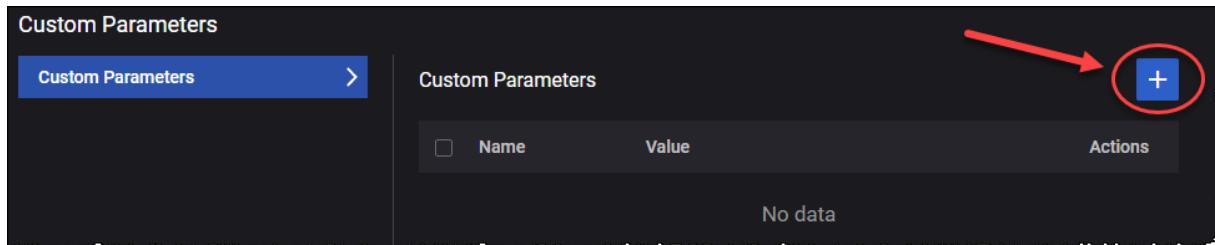
Parameter	Description
Username	Provide the username.
Password	Provide the password.
Authentication Type	Select the authentication type: <ul style="list-style-type: none"> • Digest MD5 • AKAv1

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

Custom Parameters

You can add custom parameters as follows:

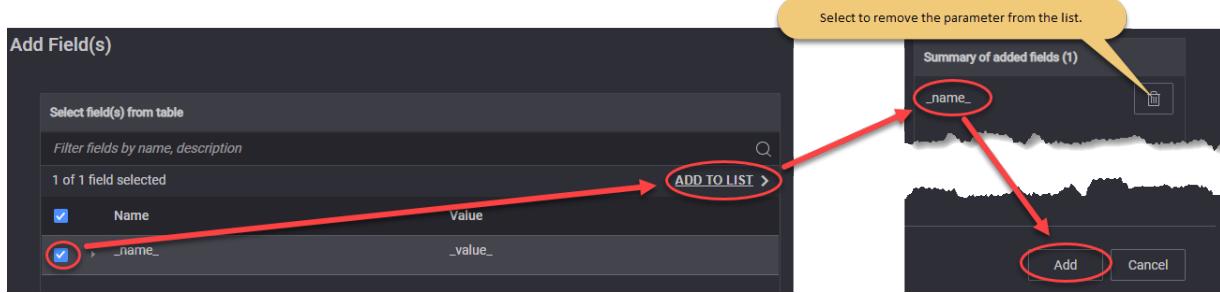
1. The Custom Parameters panel, select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom parameters are available:

Parameter	Description	Value
DelayBefore SIPInvite	Delay in miliseconds before sending SIP INVITE.	1000
DealyBeforeRTP	Delay in miliseconds before RTP session start.	0
DelayAfterRTP	Delay in miliseconds after RTP session end.	0
DeregisterLoop	Set the number of calls/loops before a SIP deregistration will be performed. Any SIP deregistration will be followed by a new SIP registration.	0
DelayBefore180	Delay in miliseconds before 180 Ringing message will be sent.	0
DelayBefore200INVITE	Delay in miliseconds before 200 OK message for INVITE will be sent.	0
debugIPSEC	Activate IPSEC debug. Please use debug only for a reduced number of simulated UEs.	0
timeoutSIP	Global timeout in miliseconds foe any SIP message. Default is set to standard 32000ms. Use this parameter to modify the default value.	32000
MaxActiveLimit	Set maximum allowed concurrent TCP connections per CPU Core. Default it is set to 8000. Please use this parameter to modify the deafult value.	8000

SIP 3GPP IPSEC

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

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

Video OTT Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	Select the value from the drop-down list: Simulated Users or Throughput .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
Advanced	Select the Open Advanced OTT button to enable and configure Advanced OTT

Parameter	Description
OTT	<u>Settings.</u>

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

Parameter	Description
Control	
Advanced Client settings	These settings are presented in the Advanced Client Settings pane.

Quality Control

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

Parameter	Description
<i>Jitter Buffer:</i>	
Initial Delay (s)	Set the number of seconds to wait before playback. The default value is 20.
Maximum Size (s)	Set the number of seconds to be buffered on the client side. The default value is 20.
MOS P.1203	Select an option from the drop-down list: Disabled or Mode 0 .
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> • Adaptive Bit Rate • Quality Predefined Levels • Lowest Quality • Highest Quality
Number of segments	This field is available and editable only when the Quality Control Mode is set to Adaptive Bit Rate .
<i>Play Profiles: The following settings are available and editable only when the Quality Control Mode is set to Quality Predefined Levels.</i>	
	Select this button to add a predefined play profile to your test configuration.
<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

Parameter	Description
	<ul style="list-style-type: none"> 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

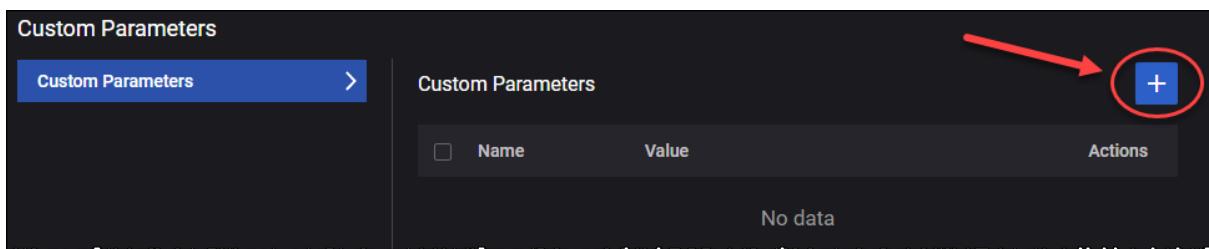
The parameters required for Advanced Client settings are presented in the table below.

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.
Enable DNS Query Per Connection	Select the check box to process only one DNS query per TCP connection.
Custom parameters	For more details, refer to Custom parameters .

Custom Parameters

You can add custom parameters as follows:

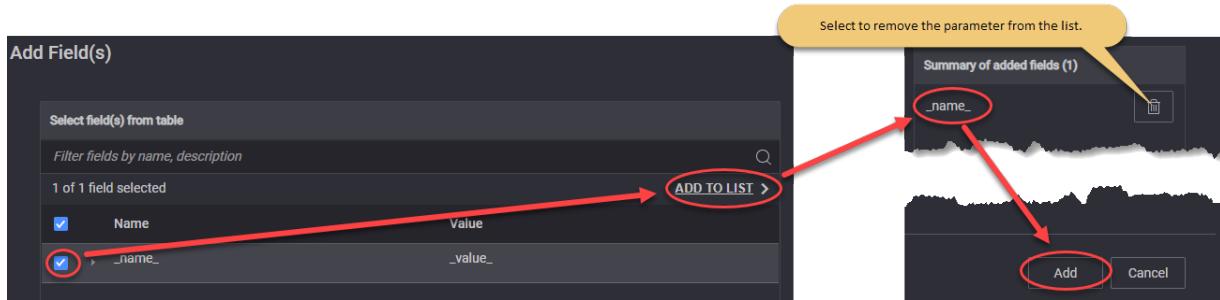
1. Select the **Open Custom Parameters** tile. The Custom Parameters panel opens.
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DNS Client Traffic

The following table describes the DNS Client Traffic parameters.

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

Parameter	Description
	<p>Refer to Flow or a description of the configuration settings for these traffic flows. Also, you can add custom parameters, based on your test configuration requirements.</p>

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Type	By default, the type is set to DNS Client .
Port	The port used by the flow.
DNS Server IP	Set the DNS server IP address.
Number of DNS servers	Set the number of DNS servers.
Hostname	Set the hostname.
Query Type	Select the query type from the drop-down list. The available options are: <ul style="list-style-type: none"> • A • AAAA • CNAME • TXT • PTR • NS
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.
QoS FlowID	Select a QoS Flow ID for this flow from the drop-down list.

Custom Parameters

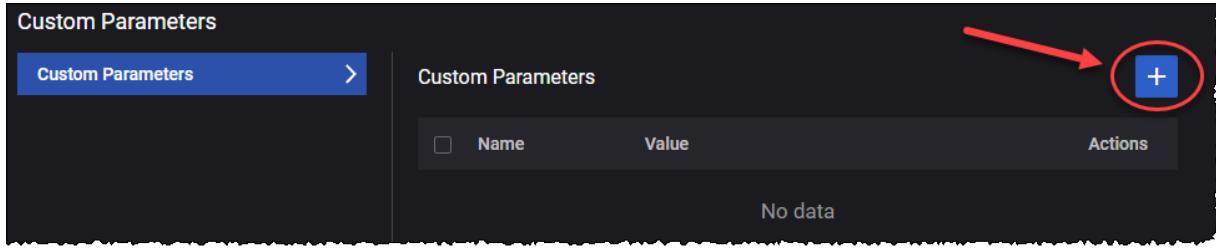
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

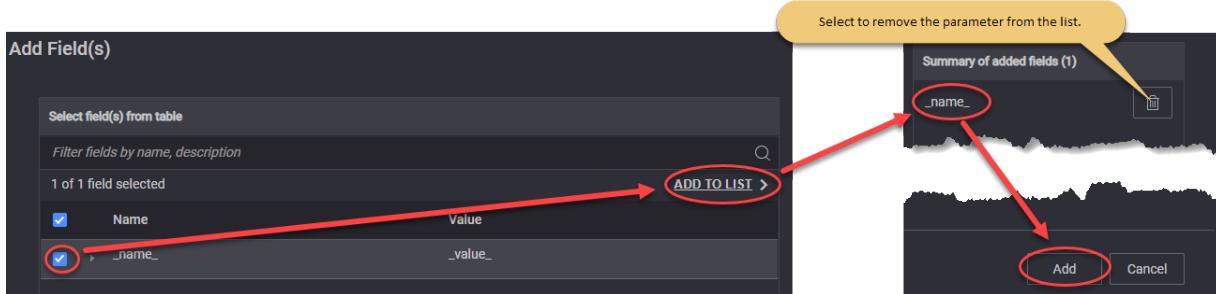
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



ICMP Client

The following table describes the ICMP Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to ICMP Client .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Traffic Flow	Refer to Traffic Flow for a description of the configuration settings for these traffic flows.

Traffic Flow

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

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

Predefined Applications Traffic

The following table describes the Predefined Flows Traffic parameters.

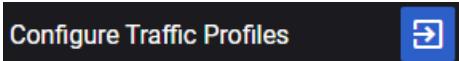
Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Simulated Users • Throughput • Connections Per Second
Throughput (kbps)	IMPORTANT This parameter is available only when Objective Type is set to Throughput . The desired throughput (in kbps) for the combined traffic flows that will be generated.
Connections Per Seconds	IMPORTANT This parameter is available only when Objective Type is set to Connections Per Second . Set the number of connections.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).

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

Traffic Profile

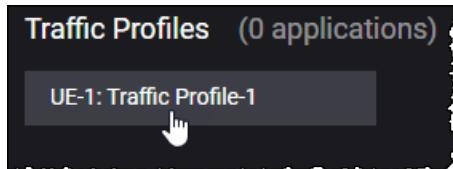
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

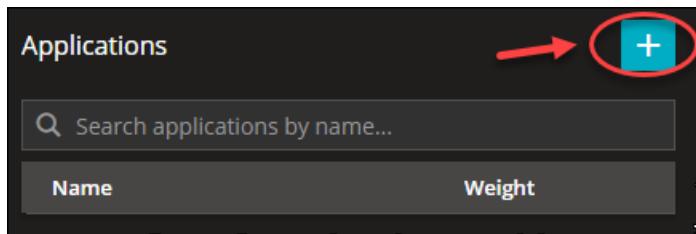
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

Applications

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

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



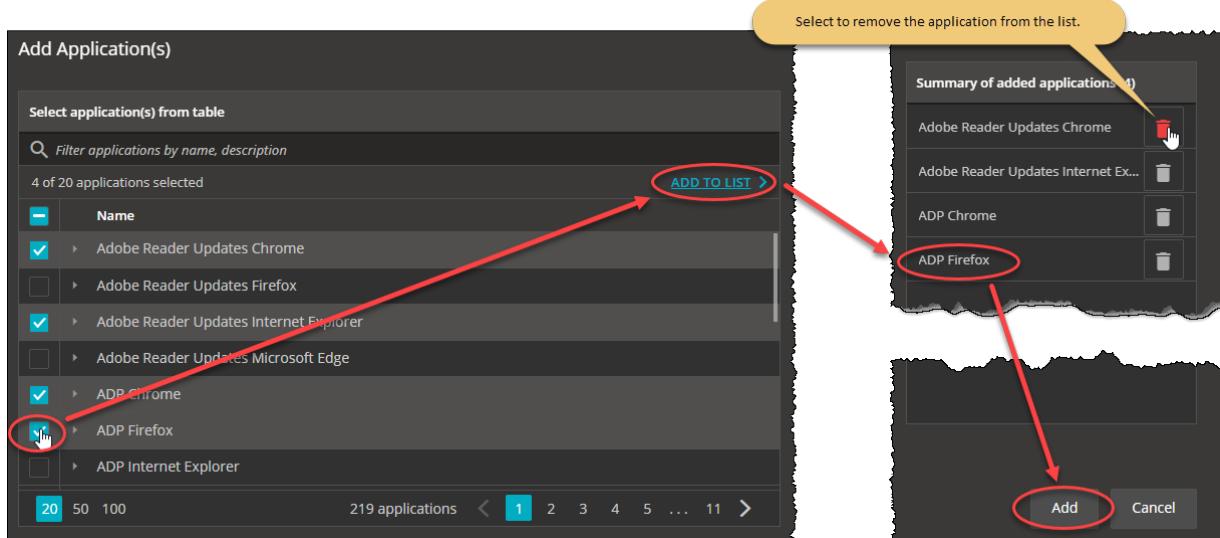
The Add Application(s) window opens.

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

NOTE

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

For example ...



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

For example ...

Applications											
Edit +											
Search applications by name...											
<table border="1"> <thead> <tr> <th>Name</th> <th>Weight</th> </tr> </thead> <tbody> <tr> <td>Adobe Reader Updates Chrome 1</td> <td>1 ▼ ▲ Edit Advanced Settings Delete</td> </tr> <tr> <td>Adobe Reader Updates Internet Exp...</td> <td>1 ▼ ▲ Edit Advanced Settings Delete</td> </tr> <tr> <td>ADP Chrome 3</td> <td>1 ▼ ▲ Edit Advanced Settings Delete</td> </tr> <tr> <td>ADP Firefox 4</td> <td>1 ▼ ▲ Edit Advanced Settings Delete</td> </tr> </tbody> </table>		Name	Weight	Adobe Reader Updates Chrome 1	1 ▼ ▲ Edit Advanced Settings Delete	Adobe Reader Updates Internet Exp...	1 ▼ ▲ Edit Advanced Settings Delete	ADP Chrome 3	1 ▼ ▲ Edit Advanced Settings Delete	ADP Firefox 4	1 ▼ ▲ Edit Advanced Settings Delete
Name	Weight										
Adobe Reader Updates Chrome 1	1 ▼ ▲ Edit Advanced Settings Delete										
Adobe Reader Updates Internet Exp...	1 ▼ ▲ Edit Advanced Settings Delete										
ADP Chrome 3	1 ▼ ▲ Edit Advanced Settings Delete										
ADP Firefox 4	1 ▼ ▲ Edit Advanced Settings 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' management interface. On the left, there's a search bar and a table listing applications with columns for Name and Weight. One row is selected, showing 'Adobe Reader Updates Chrome 1' with a weight of 1. On the right, there are two main sections: 'Application Settings' and 'Application Actions'. The 'Application Settings' section contains fields for Destination Hostname, DNN ID, and QoS Flow ID. The 'Application Actions' section contains a search bar and a table listing actions with columns for # and Name, showing 'Check For Updates' and 'Download Updates'.

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.

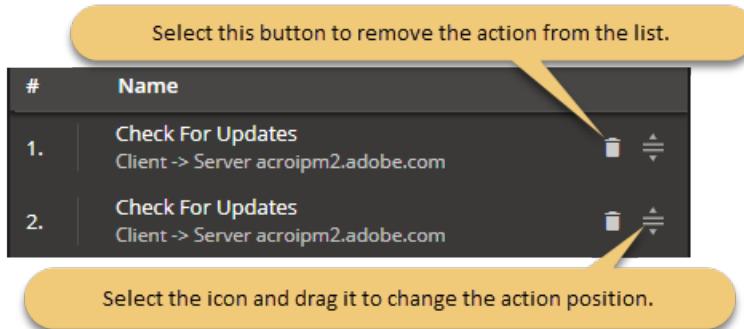
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

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:

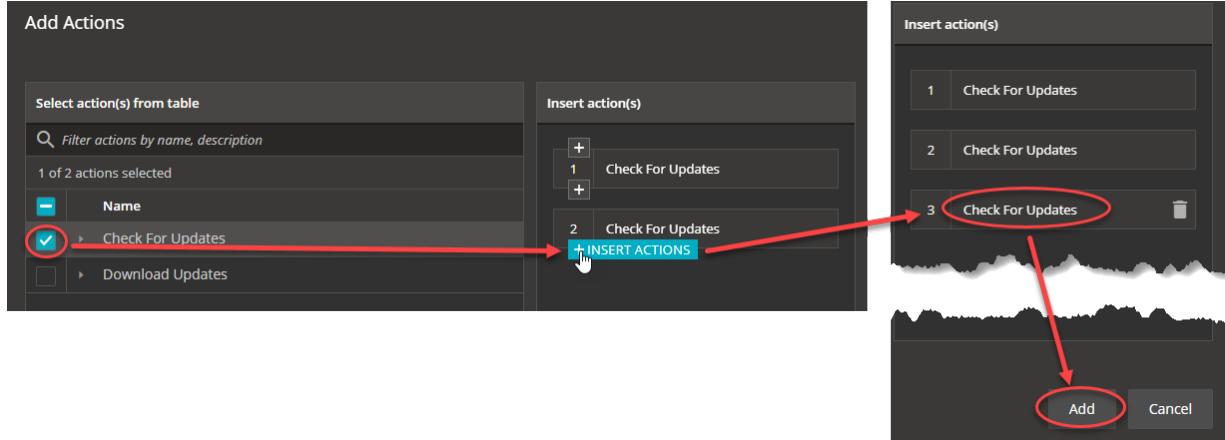
1. Use the icons available for each icon in order to remove it or to change its position in actions list.
For example ...



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 ...



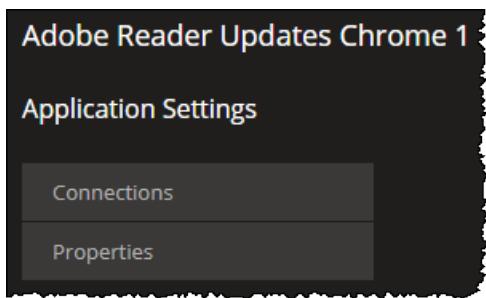
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

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.

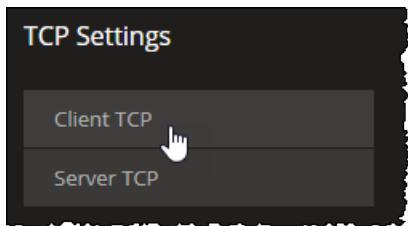
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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.



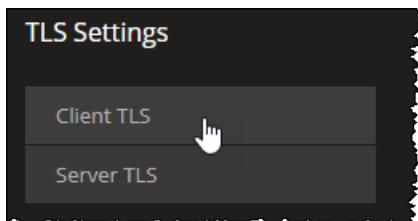
These parameters are configurable for both Client and Server settings, as presented in the following table.

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 style="text-align: center;">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.
SNI Enabled	Select the check box to enable the server name indicator. The following SNI Settings become available:
Certificate file	Select Upload to add your certificate file or Clear to remove it.
Key file	Select Upload to add your key file or Clear to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select Upload to add your DH file or Clear to remove it.
Certificate file	Select Upload to add your certificate file or Clear to remove it.
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.

RTP Settings

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

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

Capture Replay

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

The following table describes the Capture Replay parameters.

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

Parameter	Description
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.

The following table describes the Filter object parameters.

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

DN 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:

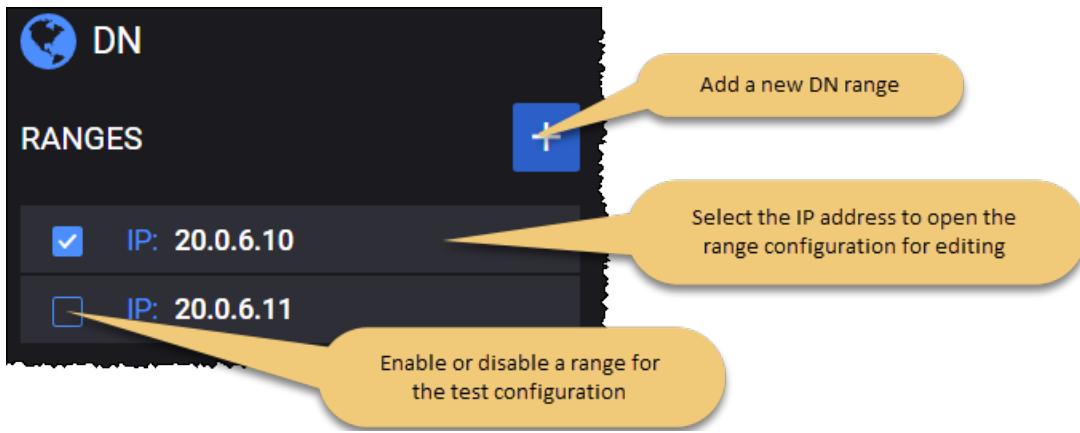
DN Ranges panel	606
DN Range panel	607
DN N6 Interface settings	608
DN routes settings	609
DN User Plane	609
DN Stateless UDP Traffic	610
DN Data Traffic	611
DN Voice Traffic	614
DN Video OTT Traffic	626
DN DNS Server Traffic	628
DN Predefined Applications Traffic	631
DN Capture Replay	631

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 **Routes Settings** to configure the route to an UE or custom 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 .
Routes Settings	These settings are described in DN routes settings .

Setting	Description
User Plane	These settings are described in DN user plane .

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
<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	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 VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

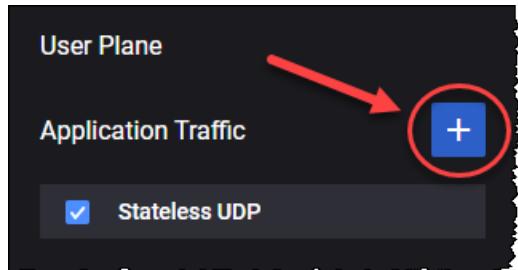
DN routes settings

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

Settings	Description
<i>Routes Config:</i>	
	Select this button to add a new route to a specific UE range or a custom one.
<i>UE Routes Config:</i>	
	Select this button to remove the route.
Route Type	Select the route type from the drop-down list. Available options: UE or Custom .
UE Range IPv4	Select the IPv4 address of the UE range from the drop-down list.
UE Range IPv6	Select the IPv6 address 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.
Destination Subnet Address	Set the destination subnet address. This parameter is available only when the route type is set to Custom .
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address. This parameter is available only when the route type is set to Custom .

DN User Plane

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



NOTE

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

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

DN Stateless UDP Traffic

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

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

Parameter	Description
	configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
Destination UE Range	Select the destination UE range from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow. When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>

DN Data Traffic

The following table describes the DN Data Traffic parameters.

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

Parameter	Description
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Application Servers	<p>Each Application Traffic entry requires an application server definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"> • To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings. • To add another application server, click the Add Server button. LoadCore will open the Server panel where you will select the server type and configure the server settings. <p>Refer to Server (below) for a description of the configuration settings required by the application server.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

Server

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

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

Custom Parameters

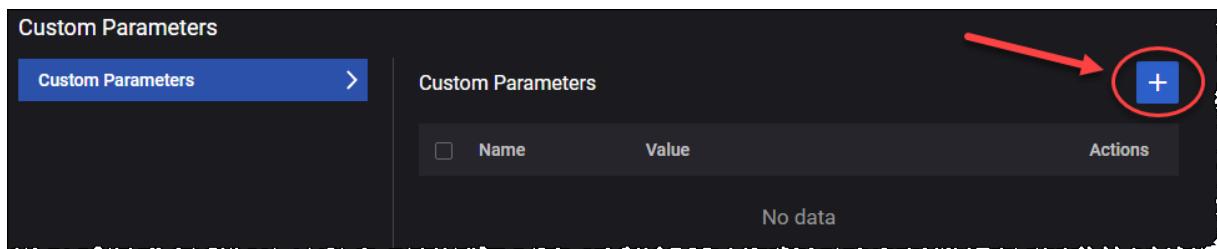
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

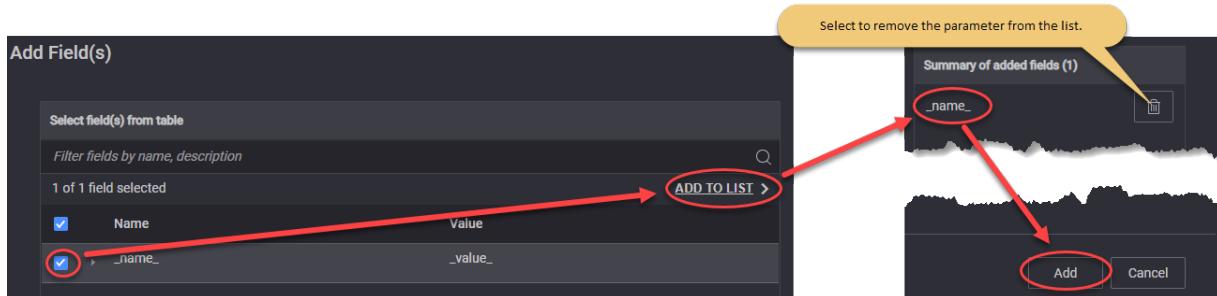
2. Select the **Add** button.



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 ...



DN Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Call Type	Select the type of call from the drop-down list.
Dial Plan:	<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

Parameter	Description
	overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security • UDP - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	For more details about these settings, refer to Media Settings .
<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.
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select the check box in order to enable this option.
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
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.

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.

Parameter	Description
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>
<i>Advanced Media Settings</i>	
Custom SDP	Select this panel to open the custom SDP settings.
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	<p>Select the template from the drop-down list:</p> <ul style="list-style-type: none"> • None • EVS/AMR IPv4

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

AMR/AMR-WB

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

EVS

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

Parameter	Description
	<ul style="list-style-type: none"> 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.

Advanced SIP Settings

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

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

SIP Custom Headers

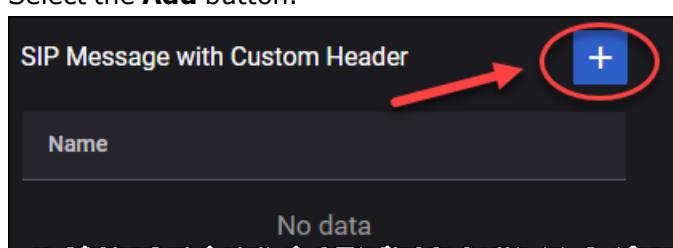
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE

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

For each message, you can:

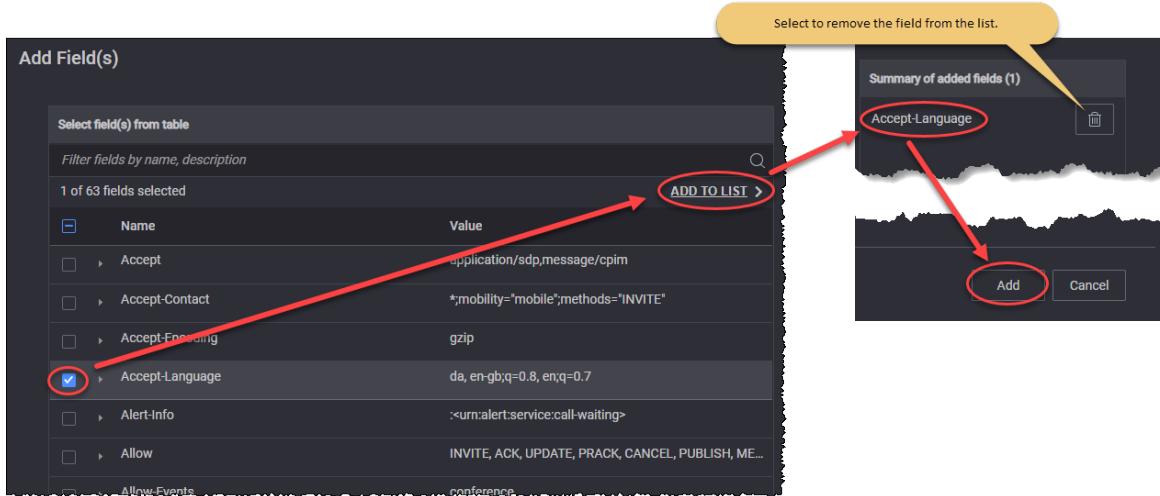
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
 - Select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom header are available:

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

Parameter	Description	Value
	IETF RFC 3310	
Call-Info	IETF RFC 3261	<http://www.example.com/alice/photo.jpg> ;purpose=icon
Content-Disposition	IETF RFC 3261	session
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:00 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC	3600

Parameter	Description	Value
	3261	
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC 4028	60
Organization	IETF RFC 3261	Keysight
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>

Parameter	Description	Value
	3327	
P-Called-Party-ID	IETF RFC 7315	sip:user1-business@example.com
P-Charging-Function-Addresses	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Charging-Vector	IETF RFC 7315	icid-value=1234bc9876e;icid-generated-at=192.0.6.8;orig- ioi=home1.net
P-Early-Media	IETF RFC 5009	supported
Permission-Missing	IETF RFC 5360	userC@example.com
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com", qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque ="", stale=False, algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice", realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",r esponse="245f23415f11432b3434341c022"
Proxy-	IETF	foo

Parameter	Description	Value
Require	RFC 3261	
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>, <sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org? Replaces=425928%40bobster.example.com.3%3Bto-tag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10

Parameter	Description	Value
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore

Parameter	Description	Value
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

SIP Authentication

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

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

DN Video OTT Traffic

The following table describes the Video OTT Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
<i>OTT Servers:</i>	
	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 • HTTP/QUIC
Port	Set the port number. 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.
Streams	Refer to Streams (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Streams

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



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

Parameter	Description
	Select this button to add a stream to your test configuration.
	Select this button to remove the stream from the test configuration.
Stream Name	Set the stream name. Each server is identified by a unique name. You can accept the value provided by 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.</i>
	Select this button to add a quality level to your test configuration.
	Select this button to remove the quality level from the test configuration.
Bitrate (kbps)	Set the value of the bitrate.
Resolution	Select the resolution from the drop-down list. Available options: QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K .
Frames per second	Set the number of frames per second.

Custom Parameters

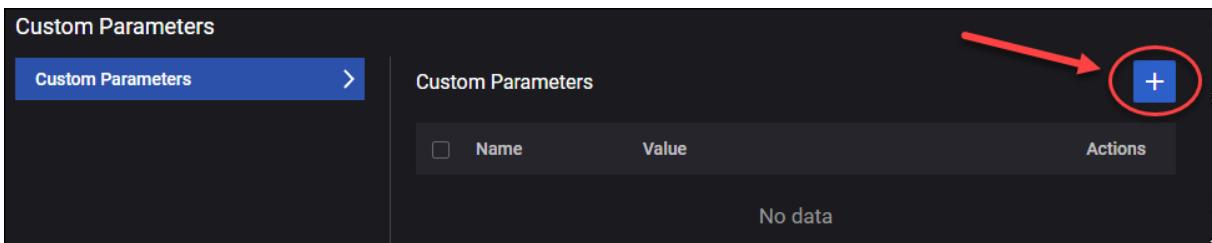
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

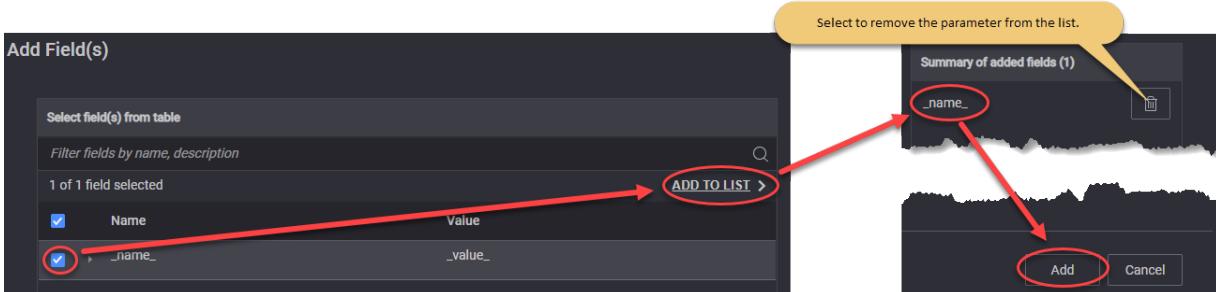
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DN DNS Server Traffic

The following table describes the DNS Server Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to DNS Server .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single,

Parameter	Description
	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>DNS Servers:</i>	
	Select this button to add an DNS server to your test configuration.
	Select this button to remove the DNS server from the test configuration.
Type	Select the type from the available options.
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
Zone Manager	<i>Refer to Zone Manager (below) for descriptions of the DNS server zones settings.</i>
Custom Parameters	<i>You can add custom parameters, based on your test configuration requirements.</i>

Zone Manager

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



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

Parameter	Description
	Select this button to add a zone to your test configuration.
	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by LoadCore or overwrite it with your own value.
Master Server	Provide the value for the master server.
Resource Records (RRs)	

Parameter	Description
	Select this button to add a resource record to your test configuration.
	Select this button to remove the resource record from the test configuration.
Type	Select the type from the drop-down list. The available options are: <ul style="list-style-type: none"> • A • AAAA • CNAME • TXT • PTR • NS
Hostname	Set the hostname.
Address	Provide the address.

Custom Parameters

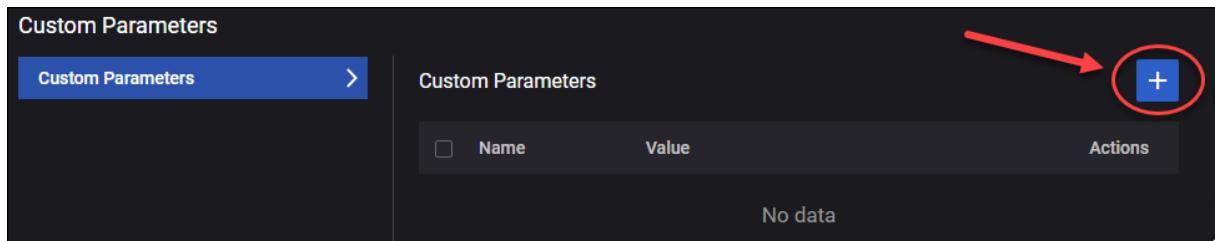
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

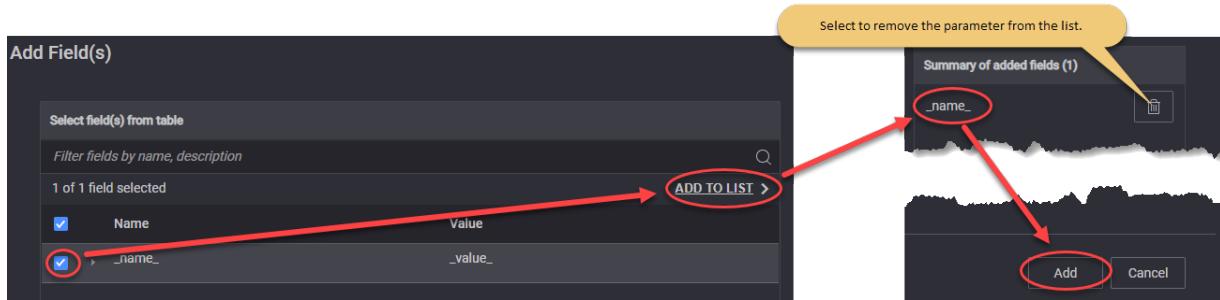
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DN Predefined Applications Traffic

The following table describes the Predefined Applications parameters.

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

DN Capture Replay

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to Capture Replay .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Capture File	It allows you to upload a capture file, using the Upload button. To remove the file, select the Clear button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to 0 for no limit. The default value is 1 .

Parameter	Description
Maximum Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Rx Timeout (ms)	Time the responder waits for packets, after the delay observed in the packet capture. The default value is 1000 miliseconds.
Delayed Tx	Prevent the packets from being sent faster than they appear to be sent in the capture file, trying to maintain the packet delays. The default value is true (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is true (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN ID	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>
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Count	The destination IP address count value.

The following table describes the Filter object parameters.

Parameter	Description
<i>Filter</i>	

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

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	635
RAN Range settings	635
RAN N3 interface settings	636
Passthrough interface settings	637

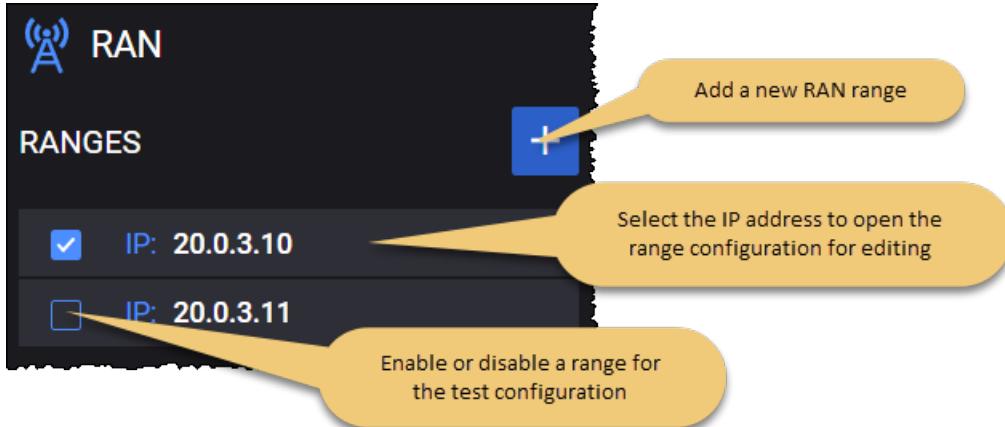
RAN Ranges panel

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.
Range Count	The number of RANs in the RAN range.

Setting	Description
<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 .
Passthrough Interface Settings	These settings are described in passthrough interface settings .

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>
VLAN ID	VLAN identifier.

Connectivity Settings	Description
VLAN TPID	VLAN tag protocol ID.

Passthrough interface settings

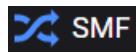
The configuration of the passthrough interface is required when passthrough is enabled in the UE settings. This interface will wait for an external traffic source.

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.

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	639
SMF Range settings	639
SMF N4 interface settings	640
SMF Uplink Paths	642

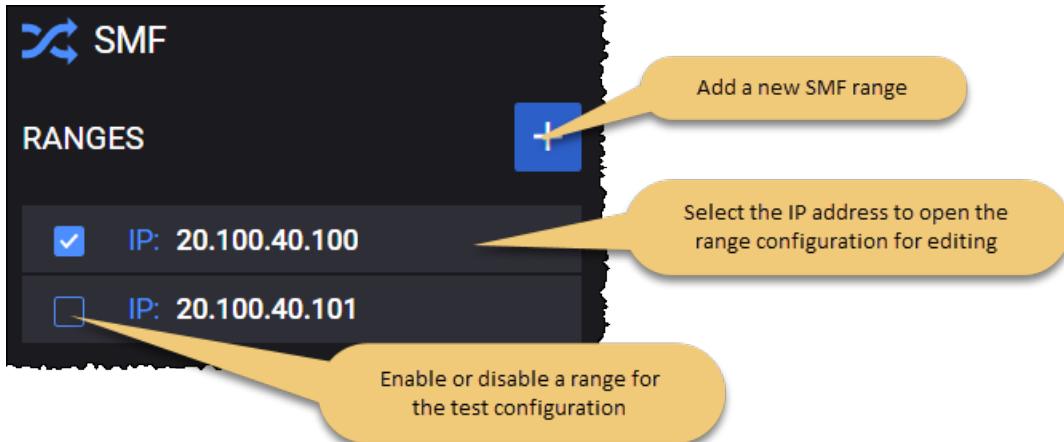
SMF Ranges panel

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>	
N4	Each SMF range requires the configuration of N4 interface settings, through which a

Setting	Description
Interface Settings	SMF instance interacts with UPF in a 5G network. These settings are described in SMF N4 interface settings .
Uplink Paths	These settings are described in SMF uplink paths .

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.
Supports PDI Optimization	The Packet Detection Information (PDI) Optimization option allows the optimization of PFCP signaling between the Control Plane and the User Plane function. This option is available only if Supports FTEID Allocation option is enabled.
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.

Setting	Description
Wait for Association Setup	The time in seconds to wait for PFPC Association setup to be initiated by UPF. The default value is 0, meaning the SMF will not wait for UPF to initiate the association. 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	The SDF describing the packet filter. Default value: <i>permit out 58 from any to assigned.</i> 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.
CP-Function SDF	The SDF describing the packet filter. Default value: <i>permit out 58 from any to assigned.</i> 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.

The following **Connectivity Settings** enable the necessary N4 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.
<i>MAC</i>	<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.
<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.
<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>

Connectivity Settings	Description
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.

Setting	Description
QoS Flows for second N9 UPF	Select the QoS Flows for the second N9 UPF.

UPF configuration settings

The configuration settings are described in the topics listed below.

Topics:

UPF Ranges panel	645
UPF Range panel	645
UPF N3 interface settings	646
UPF N4 interface settings	647
UPF N6 interface settings	649
UPF N9 interface settings	650
UPF N4u interface settings	651

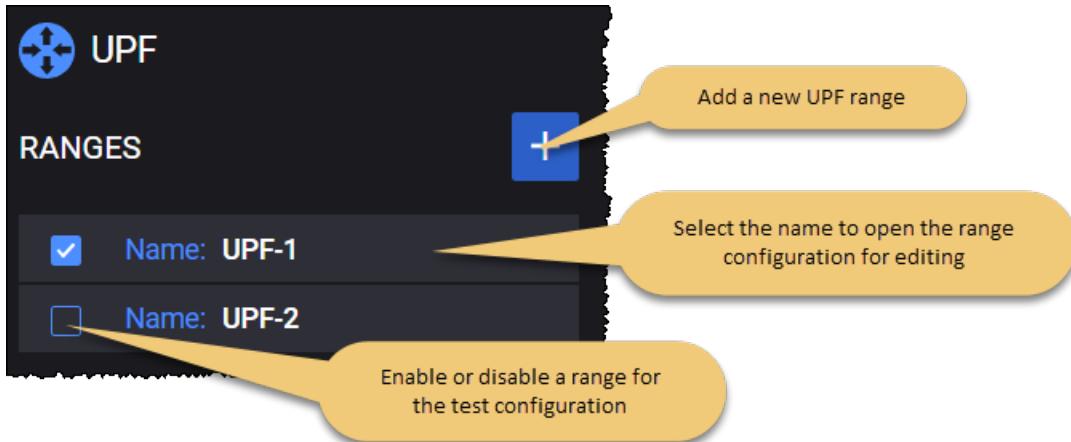
UPF Ranges panel

The **UPF Ranges** panel opens when you select the UPF 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).
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.

Setting	Description
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 .
N4 Interface Settings	N4 is the interface between the SMF and the UPF. The interface settings are described in UPF N4 interface settings .
N6 Interface Settings	N6 is the interface between the DN and the UPF. The interface settings are described in UPF N6 interface settings .
N9 Interface Settings	N9 is the interface between two UPFs. The interface settings are described in UPF N9 interface settings .
N4u Interface Settings	N4u is an interface between the SMF and the UPF. The interface settings are described in UPF N4u interface settings .

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>	<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>	

Setting	Description
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.
Supports PDI Optimization	<p>The Packet Detection Information (PDI) Optimization option allows the optimization of PFCP signaling between the Control Plane and the User Plane function.</p> <p>This option is available only if Supports FTEID Allocation option is enabled.</p>
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</i> address).

Connectivity Settings	Description
	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>
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	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.
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

Connectivity Settings	Description
	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>
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:



N4u Interface Settings

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.

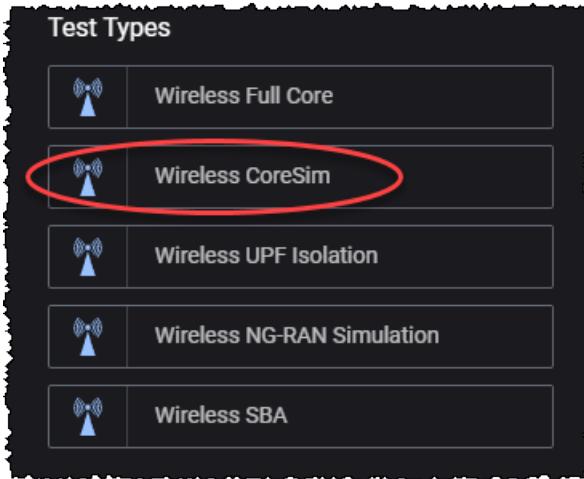
NOTE The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

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 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.

CHAPTER 11**CoreSim tests: configuration settings**

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



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

Topics:

Global Settings	658
Global Settings panel	659
Node Start/Stop Rates	659
DNS Settings	660
Advanced Settings	660
DNNs panel	663
DNN configuration settings	663
Session AMBR configuration settings	667
ePCO configuration settings	668
Traffic Control Settings configuration	668
Impairment	669
QoS Flows panel	670
QoS Flow configuration settings	670
QoS Flow Max Packet Loss Rate settings	673

QoS Flow ARP configuration settings	674
QoS Flow MBR configuration settings	674
QoS Flow GBR configuration settings	675
Milenage	675
Customer Parameters	676
CA Certificates	676
UE configuration settings	677
UE Ranges panel	678
UE Range panel	678
Range Settings	680
UE Identification settings	680
UE Security settings	681
UE Settings settings	684
UE Shared Data IDs	689
UE Subscribed AMBR settings	689
Service Area Restriction settings	690
Forbidden Areas	691
DNNs Config	692
Notifications	694
SMS Configuration	695
Equipment Status	696
Converged Charging	697
Spending Limit Control	698
Network Slicing settings	700
UE NSSAI settings	700
UDM Default NSSAI settings	701
UDM SNSSAI Mappings	702
UDR SNSSAI Settings	703
Objectives	704
Control Plane Objective	704
About primary objectives	704
Primary Control Plane Objective	706

Secondary Control Plane Objective	708
User Plane Objectives	715
Stateless UDP Traffic	717
Data Traffic	718
Voice Traffic	722
Video OTT Traffic	736
DNS Client Traffic	740
ICMP Client	743
Ping Traffic	744
Capture Replay	745
Predefined Applications Traffic	747
DN configuration settings	758
DN Ranges panel	758
DN Range panel	759
DN N6 interface settings	760
DN routes settings	761
DN User Plane	762
DN Stateless UDP Traffic	763
DN Data Traffic	764
DN Voice Traffic	766
DN Video OTT Traffic	776
DN DNS Server Traffic	779
DN Predefined Applications Traffic	781
DN Capture Replay	782
IMS configuration settings	785
CSCF Range panel	785
Media Function Range panel	786
RAN configuration settings	787
gNodeB	787
gNodeB Ranges panel	788
gNodeB Range settings	792
gNodeB node settings	793

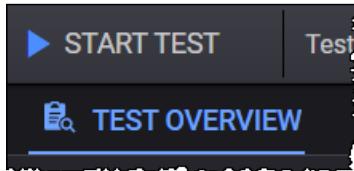
gNodeB NSSAI settings	795
gNodeB N2 interface settings	796
gNodeB N3 interface settings	800
eNodeB	804
eNodeB Ranges panel	804
eNodeB Range Settings	808
eNodeB Node Settings	809
S1-U Interface Settings	809
S1-MME Interface Settings	811
Passthrough interface settings	812
CoreSim configuration settings	815
Core settings	815
N6/SGi interface settings	816
AMF Ranges configuration settings	817
AMF node settings	819
AMF N2 interface settings	822
UPF Ranges configuration settings	823
UPF N3 interface settings	824
MME Ranges configuration settings	825
MME node settings	826
MME S1 interface settings	827
SGW Ranges configuration settings	828
SGW S1-u interface settings	829
SEG Ranges configuration settings	830
SEG interface settings	834

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:

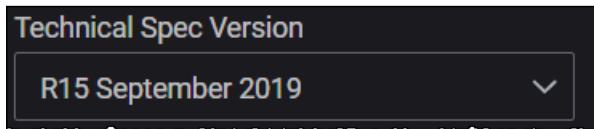


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



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	659
Node Start/Stop Rates	659
DNS Settings	660
Advanced Settings	660
DNNs panel	663
DNN configuration settings	663
Session AMBR configuration settings	667
ePCO configuration settings	668
Traffic Control Settings configuration	668
Impairment	669
QoS Flows panel	670
QoS Flow configuration settings	670
QoS Flow Max Packet Loss Rate settings	673
QoS Flow ARP configuration settings	674

QoS Flow MBR configuration settings	674
QoS Flow GBR configuration settings	675
Milenage	675
Customer Parameters	676
CA Certificates	676

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.

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

Node Start/Stop Rates

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

Setting	Description
<i>Node Start</i>	

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

DNS Settings

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

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

Advanced Settings

The following table describes the settings required to enable user plane and control plane advanced statistics.

Setting	Description
Ignore Offline Agents At Runtime	When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.
Overwrite	Enable this option to overwrite the capture size for IxStack.

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

Setting	Description
Log Tags	Select one or more tags from the drop-down list. Log Tags are used to collect specific information in the logs; they work with Debug and with Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.
Traffic Settings	<i>The settings are described here.</i>
Response Cache Settings	<i>The settings are described here.</i>

Traffic Settings

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

Setting	Description
<i>GTPU Source Port:</i>	
Start	Indicates the source port for the GTPU tunnel. By default, the registered UDP port for GTPU is 2152.
Count	Set the count value.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable RTP.
Enable ICMP Responses	Select this option to enable it. This will permit requests and responses to ICMP packets on subscribers addresses (it will have a significant memory impact on server nodes - AMF, UPF).
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.

Response Cache Settings

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

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

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

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

DNNs panel

To access the DNN configuration settings, select **DNNs** from the the **Global Settings** panel. 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	663
Session AMBR configuration settings	667
ePCO configuration settings	668
Traffic Control Settings configuration	668

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
DNN:	
DNN	<p>Enter the DNN value for this DNN definition. For example: <code>dnn.keysight.com</code>. 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 <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 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>
PDU Type	Select the desired PDU type: IPv4, IPv6 or IPv4v6.
Allowed	Select the allowed session types from the drop-down list: IPv4 IPv6, IPv4, IPv6,

Setting	Description
Session Types	UNSTRUCTURED, ETHERNET, or all.
Default Session Type	Select the default session type from the drop-down list: IPv4 IPv6, IPv4, IPv6, UNSTRUCTURED, 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.</p>
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) that had been allocated to the UE. SSC Mode 3: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Default SSC Mode	<p>Select the desired default SSC mode for this DNN.</p> <p>The SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session.</p>
Allowed Services	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 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	Enable this option if the UE subscription data indicates support for interworking

Setting	Description
Interworking	with EPS for this DNN.
Is Local Area DN	<p>Enable 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	Enable this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.
Subscriber Spending Limits	Enable this option if the DNN will support PDU session policies that are based on subscriber spending limits.
Offline	Enable this option if the DNN will support the offline charging method for PDUs sessions.
Online	Enable this option if the DNN will support the online charging method for PDUs sessions.
Is Emergency DNN	When this option is enabled, if an UE range has mapped this type of DNN, it will perform an emergency PDU Session.
MPS Priority	Enable this option if the DNN will support subscription to MPS priority service. The priority applies to all traffic on the PDU Session.
MPS Priority Level	Specify the Multimedia Priority Services (MPS) priority level. This is the relative priority level for MPS.
IMS Signaling Priority	Specify the IP Multimedia Subsystem (IMS) signaling priority. This value indicates subscription to IMS signaling priority service. The priority applies only to IMS signaling traffic.
Access Network Instance	<p>Set the access network instance.</p> <p>It represents the value to be sent in the Network Instance IE when the source interface is set to Access.</p>
Core Network Instance	<p>Set the core network instance.</p> <p>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.</p>
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.

Setting	Description
Guaranteed Bit Rate Downlink	Specify the guaranteed bit rate for the downlink traffic.
Session AMBR	<i>Select this option to open a new panel that contains the Session AMBR settings. These settings are described in Session AMBR configuration settings.</i>
ePCO	<i>Select this option to open the extended protocol configuration options panel. These settings are described in ePCO configuration settings.</i>
Traffic Control Settings	<i>Select this option to open the traffic control settings panel. These settings are described in Traffic Control Settings configuration.</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](#).
- The DNN's Session AMBR settings, described below.

About Session AMBR ...

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

The following tables describes the Session AMBR configuration settings.

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

ePCO configuration settings

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	Add DNS Server IPv4 Address Request or DNS Server IPv6 Address Request in the Extended Protocol Configuration Options IE included in PDU Session Establishment Request message. If required, enable this option.
Request P-CSCF IP address	Add P-CSCF IPv4 Address Request or P-CSCF IPv6 Address Request in the Extended Protocol Configuration Options IE included in PDU Session Establishment Request message. If required, enable this option.
Request IPv4 Link MTU	Add IPv4 Link MTU Request in the Extended Protocol Configuration Options IE included in PDU Session Establishment Request message. If required, 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. Select the check box to enable it.
Suspend Traffic Interval(s)	Set the value (in seconds) for this parameter.

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

Impairment

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

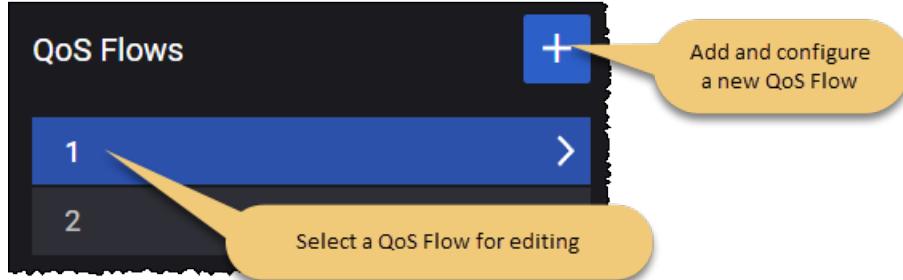
Setting	Description
<i>Impairment Profiles:</i>	
	Select the Add impairment profile button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the Delete impairment profile button to remove the profile from your test configuration.
Name	Each impairment profile is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Action Type	Select an option from the drop-down list. The available option is: Custom script .
Script file	This parameter is available only when Action Type is set to Custom script . It allows you to add a custom script, using the Upload button. To remove the script, select the Clear button.

QoS Flows panel

The 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	670
QoS Flow Max Packet Loss Rate settings	673
QoS Flow ARP configuration settings	674
QoS Flow MBR configuration settings	674
QoS Flow GBR configuration settings	675

QoS Flow configuration settings

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

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

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

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

Setting	Description
Type	<p>IMPORTANT This parameter is available only if the Is Default option is not selected.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> • Data - 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.
Network Initiated Flow	<p>IMPORTANT This parameter is available only if the Is Default option is not selected.</p> <p>Select the associated check box to enable this option.</p> <p>The following fields are displayed:</p> <ul style="list-style-type: none"> • <i>Delay After Initial Registration (s)</i> - set the value for this parameter. • <i>Interval between Create and Delete (s)</i> - set the value for this parameter. • <i>Iterations</i> - set the value for this parameter.
QFI	<p>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.</p>
5QI	<p>Specify the 5QI value (decimal number).</p> <p>5G QoS Identifier (5QI) is a scalar that is used as a reference to 5G QoS characteristics defined in TS 23.501, clause 5.7.4. These are access node-specific parameters that control QoS forwarding treatment for the QoS Flow (such as scheduling weights, admission thresholds, queue management thresholds, link layer protocol configuration, among others). Standardized 5QI values have a one-to-one mapping to a standardized combination of 5G QoS characteristics as specified in TS 23.501, table 5.7.4-1.</p>
5QI Priority Level	<p>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.</p>
Resource Type	<p>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.</p>
Averaging Window	<p>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</p>

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

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

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

QoS Flow MBR configuration settings

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

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

Setting	Description
<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.

Milenage

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

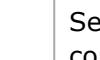
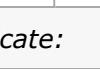
Setting	Description
R4	<p>Set the R4 value (integer type).</p> <p>Default value: 64.</p>
C5	<p>Set the C5 value (string type).</p> <p>Default value: 00000000000000000000000000000008.</p>
R5	<p>Set the R5 value (integer type).</p> <p>Default value: 96.</p>

Customer Parameters

The section allows you to use custom parameters. When **Use Custom Parameters** is enabled, you can use the text section below to add the custom parameters.

CA Certificates

The following table describes the settings required for CA certificates upload.

Setting	Description
<p><i>CA Certificates:</i></p>	
	Select the Add CA Certificate button to add a new certificate to your test configuration.
<p><i>CA Certificate:</i></p>	
	Select the Delete CA Certificate button to remove the certificate from your test configuration.
Name	Each certificate is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Certificate File (.crt)	It allows you to add the certificate from the storage location, using the Upload button. To remove the script, select the Clear button.

UE configuration settings



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

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

The configuration settings are described in the topics listed below.

Topics:

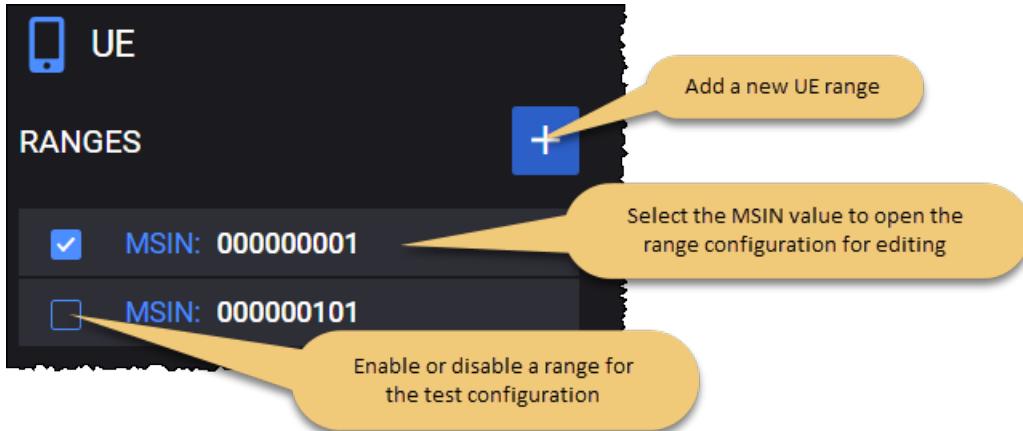
UE Ranges panel	678
UE Range panel	678
Range Settings	680
UE Identification settings	680
UE Security settings	681
UE Settings settings	684
UE Shared Data IDs	689
UE Subscribed AMBR settings	689
Service Area Restriction settings	690
Forbidden Areas	691
DNNs Config	692
Notifications	694
SMS Configuration	695
Equipment Status	696
Converged Charging	697
Spending Limit Control	698
Network Slicing settings	700
UE NSSAI settings	700
UDM Default NSSAI settings	701
UDM SNSSAI Mappings	702
UDR SNSSAI Settings	703

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

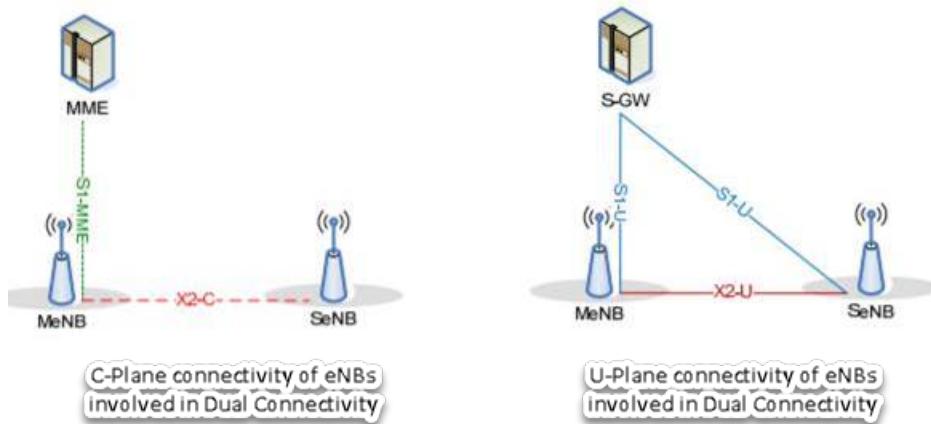
When you select an MSIN from the UE **Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- Delete the UE range from the test configuration.
- Configure the *Range Count*.
- Select the *Parent NG-RAN* for the UE range.
- Select a *Secondary Node*.
- Access the detailed UE configuration settings (Range Settings, Network Slicing, Objectives).

UE range controls and settings

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

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



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

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

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

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

Through E-RAB modification 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** option must be enabled on the QoS flows tab, on each bearer that needs to use the NR resources. The traffic will be moved to NR bearers as soon as the bearer configured to support is successfully setup.

Known limitations:

- Application Traffic is not supported on Dual Connectivity bearers.

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Range Count	Enter the number of simulated UEs required for the range.

Setting	Description
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 used for Option 3x and Dual Connectivity NR-NR features. Select the secondary node from the drop-down list.

Range Settings

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

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

UE Identification settings	680
UE Security settings	681
UE Settings settings	684
UE Shared Data IDs	689
UE Subscribed AMBR settings	689
Service Area Restriction settings	690
Forbidden Areas	691
DNNs Config	692
Notifications	694
SMS Configuration	695
Equipment Status	696
Converged Charging	697
Spending Limit Control	698

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.

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

UE Security settings

Each UE range requires security settings for subscriber authentication and subscriber privacy. In the 5G system, the SUbscription Permanent Identifier (SUPI) is a globally unique identifier allocated to each subscriber. The serving network must authenticate the SUPI in the process of authentication and key agreement between UE and network. The serving network authorizes the UE through the subscription profile obtained from the home network; this UE authorization is based on the authenticated SUPI.

The SUPI is never transferred in clear text over the 5G-RAN; instead, the SUCI is used. The SUbscription Concealed Identifier (SUCI) is a privacy-preserving identifier containing the concealed SUPI. In the 5G core network, only the UDM has authority to deconceal the SUCI.

For detailed information, refer to 3GPP TS 33.501 (Security architecture and procedures for 5G System).

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

Setting	Description
K	<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 own choosing.</p>

Setting	Description												
K Increment	The number used to increment the K value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same K value.												
Configure OP / OPc / TOP / TOPc	Select the operator-specific authentication value.												
OP	<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	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.												
TOP	A 256-bit operator variant algorithm configuration field used by the TUAK authentication algorithm.												
TOPc	A 256-bit value derived from TOP and K used by the TUAK authentication algorithm.												
TOPc Increment	The number used to increment the TOPc value for each subsequent UE in the range. A value of zero indicates that each UE in the range uses the same TOPc value.												
SUCI Protection Scheme	<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 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).												

Setting	Description
Home Network Public Key ID	The Home Network Public Key Identifier that will be used to indicate which public/private key pair to use for SUPI protection and deconcealment of the SUCI.
Ephemeral Public Key	The ephemeral public key that will be used for computing a fresh SUCI on the UE side and for deconcealing the SUCI on the home network side.
Ephemeral Private Key	The ephemeral private key that will be used for computing a fresh SUCI on the UE side.
Routing Indicator	<p>The Routing Indicator that is used in the construction of the SUCI.</p> <p>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.</p>
RAND	<p>A hexadecimal number that represents the 128-bit random challenge.</p> <p>You can accept the value generated by LoadCore, or enter of a RAND value of your own choosing.</p>
RAND Increment	Specify the RAND increment value.
AUTN	The AUthentication TokeN (AUTN) to use when authenticating the UEs in this range.
Authentication Type	<p>Select the Authentication Method to use in the authentication procedures for this range of UEs.</p> <p>In the current release, 5G-AKA is the only supported Authentication Type.</p>
Integrity Protection Maximum Uplink Data Rate	Select a value from the drop-down list: <ul style="list-style-type: none"> • 64 kbps • Full Data Rate
Integrity Protection Maximum Downlink Data Rate	Select a value from the drop-down list: <ul style="list-style-type: none"> • 64 kbps • Full Data Rate

UDM User Plane Security Profile

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

Parameter	Description
	Select the Add Security Profile button to add a new profile to your test configuration.

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

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

NOTE

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

UE Settings settings

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

Setting	Description
<i>Settings:</i>	
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. Applicable to simulated UDM NF.
Subscribed Registration Timer (s)	The Periodic Registration timer value for this range of UEs. The AMF allocates a periodic registration timer value to the UE based on local policies, subscription information and information provided by the UE. After the expiry of this timer, the UE performs a periodic registration.

Setting	Description
	Applicable to simulated UDM NF.
Active Time (s)	The subscribed Active Time for Power Saving Mode (PSM) UEs.
RAT Restrictions	<p>UE Mobility Restrictions include RAT restrictions, which define the 3GPP Radio Access Technologies (one or more) that a UE is not allowed to access in a PLMN. The options available in LoadCore are: NR, E-UTRA, WLAN, and Virtual.</p> <p>Applicable to simulated UDM NF.</p>
Set ESM Information Transfer Flag	<p>By default, this option is enabled.</p> <p>This option controls the value of the <i>ESM information transfer</i> flag from InitialUEMessage/AttachRequest 4G message.</p> <p>When this option is disabled, the UE/eNodeB will set the flag <i>ESM information transfer</i> to <i>False</i> and MME will not send DownlinkNASTransport/ESM information request.</p>
Switch Off Deregistration/Detach	When this option is enabled, the Deregistration Request/Detach messages will use a deregistration/detach type of Switch-off. When the Deregistration/Detach type is switch-off, the AMF/MME does not send the Deregistration/Detach Accept message back to the UE.
PDU Session Release Before Deregistration	When this option is enabled, the UE will release PDU sessions before deregistration.
Enable Periodic Registration Update	<p>By default, this option is not enabled.</p> <p>If the periodic registration functionality is disabled, the UE will ignore the T3512 timer received in the Registration Accept and will not send any Periodic Registration Update request.</p> <p>During the Initial Registration, the AMF sends in the Registration Accept a T3512 timer, which consists of a Unit-Value pair. For example, a value of 30 and unit of 10min means 300 minutes.</p> <p>The T3512 timer can be overridden by subsequent Registration Accept messages. If T3512 is 0 or Disabled, no periodic registration should be performed. If no T3512 value is present in the Registration Accept message, the last known T3512 value is used. If a T3512 was never transmitted by the AMF, the default value of 54 minutes will be used.</p> <p>The T3512 timer is triggered when the UE enters idle. If the UE exits the idle state, the T3512 timer is stopped. When the UE enters again in idle, the T3512 timer is restarted.</p> <p>While the UE is in idle mode, when the T3512 timer expires:</p> <ul style="list-style-type: none"> • If the UE is not registered for emergency services, the UE initiates a Periodic Registration Update procedure and restarts the T3512 timer. • If the UE is registered for emergency services, the UE locally de-

Setting	Description
	registers and the AMF locally de-registers the UE.
Delay Before PDU Session Creation (ms)	The time that will elapse before the UEs in this range begin creating PDU sessions after successful Registration.
Delay Before Deregister (ms)	The time that will elapse between PDU Session Release Complete and UE initiated Deregistration Request messages.
Delay Before Handover Notify (ms)	The time to wait before handover notification.
Delay Before Paging (ms)	The time to wait before paging, after UE enters idle.
Paging Storm Iterations	The number of times the UE will be paged.
Paging Storm Interval (ms)	The delay between paging messages, in milliseconds.
Check AUTN	<p>By default, this option is disabled.</p> <p>When the option is enabled, then UE will check the value of AUTN in the <i>Authentication Request</i> messages and it will reply with <i>Authentication Failure (MAC failure)</i> in case of different MAC values or with <i>Authentication Failure (Synch failure)</i> in the case the sequence number computed using the AUTN value is invalid.</p>
Unsolicited Router Advertisement	Select to enable this option.
AMF Force Identification During Registration	This option will force the AMF to always trigger the "Identification Procedure" to get the identity of the UE. When the NG-RAN node receives this request, it responds with the IMEISV or the SUCI.
Always Include Uplink Data Status IE in Service Request Message	The UE will always include the Uplink Data Status IE for a Service Request message, not only if it has pending data.
Enable Passthrough	<p>Select this option to enable passthrough and any interface.</p> <p>Applicable to all passthrough topologies (UE/gNB or UPF).</p> <p>Applicable to either direction: GTPu to IP or/and IP to GTPu.</p>
Attach/Register with GUTI	When the Primary Objective type is Subscribers Per Second, enabling this option will trigger a Registration/Attach Request with the type of user identity set to temporary identity (GUTI). When option is not enabled, the type of user identity in the Registration/Attach Request will be permanent identity.
Force Emergency	When this option is enabled, the UE will perform an Emergency

Setting	Description
Registration	<p>registration (instead of Initial Registration).</p> <p>Only the primary objective's DNNs are taken into account when deciding if the UE performs an emergency registration. When the <code>dnnIdsToActivate</code> is present but empty in the primary objective, the Emergency Registration will not be performed even if there is a Secondary Objective that uses an emergency DNN.</p>
Identity Type for Emergency Registration	Select an option from the drop-down list. Available options: SUCI or IMEISV .
Support SMS	<p>When this is selected, a flag will be added in the Registration message advertising UE support for SMS over NAS feature.</p> <p>This feature is currently available on gNB N1N2 interface but not on the Full Core AMF, so the AMF needs to be set as DUT.</p>
Delay Before Indirect Forwarding Cleanup (ms)	The time that will elapse before indirect forwarding cleanup. The delay is calculated from the UE Context Release.
Send Native GUTI During IRAT Mobility Registration	Enable this option to send native GUTI during IRAT mobility registration.
Authentication During Mobility Registration	<p>Select a value from the drop-down list:</p> <ul style="list-style-type: none"> • Never: Authentication is not performed during mobility registration. • Always: Authentication during mobility registration is always performed. • No Native Context: Authentication during mobility registration is performed only when the UE does not hold a native 5G security context.
Update GUTI in TAU	Select to enable this option.
<i>Access and Mobility Policy:</i>	
Subscription Categories	<p>Select the desired Subscription Category for this range of UEs.</p> <p><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).</p> <p>Applicable to simulated UDR NF.</p>
Radio Capability	
UE Radio Capability IE Value for LTE	The UE radio capability IE value that will be included UE Capability Info Indication message.

Setting	Description
UE Radio Capability IE Value for NR	The UE radio capability IE value that will be included UE Capability Info Indication message.
Send UE Capability IE Indication after Initial Context Setup	Enable this option to sent UE capability IE indication after initial context setup.
Trigger UE Radio Capability Check Procedure after Registration	This option will trigger from CoreSim the UE radio capability check procedure after registration in 5G or UE radio capability match procedure after attach in 4G.
<i>Location Reporting</i>	<i>Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).</i>
Reporting Type	<p>Select the value from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • Direct - If the test timeline is long enough, the AMF generates n LocationReportingControl messages at every m seconds from the moment Registration Complete message is received by the AMF (n is the value configured for Number of Repeats and m is the value of Interval Between Requests). • Change of Serving Cell - In case of Handover with AMF change, if Change of Serving Cell is selected, after handover, the new AMF will send a LocationReportingControl message to the NG-RAN.
Interval Between Requests (seconds)	Set the time interval between requests.
Number of Repeats	Set the number of repeats.
Start Time (seconds)	The number of seconds after successful attach when the AMF sends a LocationReportingControl message (event-type: change-of-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).
<i>SMF Initiated PDU Session Release</i>	<i>Select the check box to enable this option.</i>
Time to Wait before SMF Initiated PDU Session Release (s)	Time in seconds to wait before SMF initiated PDU session release.
DNNs	<p>Select the DNNs from the drop-down list. The available options are:</p>

Setting	Description
	<ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list.
<i>Network Initiated Deregistration</i>	<i>Select the check box to enable this option.</i>
Time to wait before Network Initiated Deregistration (s)	Time in seconds to wait before network initiated deregistration.
Set Reregistration Required Flag in Deregistration Request Message	Enable this option to set a required reregistration flag in the deregistration request message.
<i>AMF Initiated UE Context Release</i>	<i>Select the check box to enable this option.</i>
Time to Wait before AMF Initiated UE Context Release (s)	Time in seconds to wait before AMF initiated UE context release.

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.

Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.

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. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.

Setting	Description
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. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.
Subscribed AMBR Downlink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.

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.

Use the settings described below to configure service area restrictions for a UE range. Applicable to simulated UDM NF, part of the UE subscription Access and Mobility Data.

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.

Setting	Description
<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 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.

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.

Setting	Description
	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 additional DNN configurations. Select the Add DNNs Config button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the Delete DNN Config button to delete this DNN config from your test configuration.
SSC Mode	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved. SSC Mode 2: The network may release the connectivity service delivered to the UE and release the corresponding PDU Sessions. The release of the PDU induces the release of the IP addresses (IPv4, IPv6, IPv4v6) that had been allocated to the UE. SSC Mode 3: Changes to the user plane can be visible to the UE, while the network ensures that the UE suffers no loss of connectivity. A connection through a new PDU Session Anchor point is established before the previous connection is terminated in order to allow for better service continuity. The IP address (IPv4, IPv6, IPv4/v6) is not preserved in this mode when the PDU Session Anchor changes.
Session ID	Provide the session ID value.
DNN	Select one of the previously-defined DNNs from the drop-down list.
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 LoadCoresimulates the SMF.

Setting	Description
	IP address is also used to create UE Routes from DN.
Local IPv4 Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Local IPv4 Address Increment	The value by which the IP addresses will be incremented.
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 LoadCoresimulates the SMF. IP address is also used to create UE Routes from DN.
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.
Local IPv6 Address Increment	The value by which the IP addresses will be incremented.
Configure S-NSSAI:	<i>When this check-box is selected, you can configure which slice (S-NSSAI) to be send in PDU Session Establishment messages. If the check-box is not selected, the first slice from Allowed NSSAI list (received in Registration Accept) is used in PDU Session Establishment message.</i> NOTE <i>This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</i>
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	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: <ul style="list-style-type: none"> if the check-box is not selected, the UE will not send any slice in PDU Session Establishment message (as the slice selected from the above list is not part of Allowed NSSAI). if the check-box is selected, the UE will use the slice selected from the above list, although it is not part of Allowed NSSAI. 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.
<i>Secondary Authentication:</i>	
Method type	The following options are available: <ul style="list-style-type: none"> None EAP-TTLS (Extensible Authentication Protocol – Tunnelled Transport)

Setting	Description
	Layer Security) <ul style="list-style-type: none"> • CHAP (Challenge-Handshake Authentication Protocol) • PAP (password Authentication Protocol)
<i>EAP-TTLS Auth Method:</i>	
CA Certificate	Provide the client certificate.
Tunneled Authentication Method	Select the tunneled authentication method: <ul style="list-style-type: none"> • PAP • CHAP
Password	Provide the password.
Send User Identity	By default, this option is disabled. Enabling this option will add SM PDU DN Request Container IE (Authentication Identity) to the PDU Session Establishment Request message send by NG-RAN.
<i>Chap Auth Method:</i>	
User	Provide the user.
Secret	Provide the password.
<i>PAP Auth Method:</i>	
User	Provide the user.
Password	Provide the password.

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 (ms)	The delay in milliseconds between Policy Data Subscriptions and Policy Data Change Notification.
<i>Policy Data:</i>	
Enable	Enable subscription to policy data notifications for the UE range.

Setting	Description
notification	
SM Policy Data json	Paste your policy data JSON file into the field.
<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

Setting	Description
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.
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	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> • SMS-MO: Mobile Originated. The UE range originates (sends) SMS messages. • SMS-MT: Mobile Termintated. The UE range waits for delivery of SMS messages.

Equipment Status

The Equipment Status lets user configure blocked or greylisted ranges of UEs using the IMEI. Applicable to simulated 5G-EIR Network Function.

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.

Setting	Description
Step	Set the step for the greylisted subscribers range.

Converged Charging

Applicable to simulated CHF Network Function. The following table describes the UE **Converged Charging** settings.

Setting	Description
Validity Time	The validity of the granted quota for a given category instance.
Quota Holding Time	A quota expiry time, when no traffic associated with the quota is observed for the value indicated by this attribute.
Time Quota Threshold	A time quota below this threshold will trigger a quota re-authorization.
Volume Quota Threshold	A volume quota below this threshold will trigger a quota re-authorization.
Unit Quota Threshold	A units quota below this threshold will trigger a quota re-authorization.
Notification Timer	Duration in milliseconds after which the CHF will notify CTF about quota re-authorization.
Enable Subscription Termination Timer	Select this option to enable the subscription termination timer.
Trigger Subscription Termination (ms)	Set the value for this parameter.
<i>Total Available Units Per PDU Session:</i>	<i>Holds the maximum amount of units to be granted per PDU session per charging session.</i>
Total Time	Set the total time value.
Total Volume	Set the total volume value.
Total Uplink Volume	Set the total uplink volume value.
Total Downlink Volume	Set the total downlink volume value.
Total Service Specified Units	Set the total service specified units value.
<i>Default Granted Units Per Charging Data Request:</i>	
Time	Set the time value.

Setting	Description
Volume	Set the volume value.
Uplink Volume	Set the uplink volume value.
Downlink Volume	Set the downlink volume value.
Service Specified Units	Set the service specified units value.

Spending Limit Control

Applicable to simulated CHF Network Function. The following table describes the UE **Spending Limit Control** settings.

Setting	Description
Enable Notify Timer	Use this option to enable 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	Use this option to enable 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	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.
Policy Counters	<i>These settings are described here.</i>
Notify Policy Counters	<i>These settings are described here.</i>

Policy Counters

Applicable to simulated CHF Network Function. The following table describes the **Policy Counters** settings.

Setting	Description
<i>Policy Counters:</i>	

Setting	Description
	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.
<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>	

Setting	Description
	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 Counter Status	Enter the policy counter status (as a string value). For example: <i>120Mbps</i> .
Activation Time	Enter the activation time (as a DateTime value) for this status value. For example: <i>2020-12-31 11:59:59</i> .

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	700
UDM Default NSSAI settings	701
UDM SNSSAI Mappings	702
UDR SNSSAI Settings	703

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 NSSAI slices are the ones supported and requested 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 **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.
SST	The Slice/Service Type (SST) value.
SD	The Slice Differentiator (SD) value for this S-NSSAI.
Mapped	The Mapped Slice/Service Type (SST) value for this S-NSSAI.

Setting	Description
SST	
Mapped SD	The Mapped Slice Differentiator (SD) value for this S-NSSAI.
DNNS	The Subscription Information for each S-NSSAI may contain a Subscribed DNN list. Select all DNNs required to be activated in this S-NSSAI (via multiple PDU Sessions).

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.

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	704
About primary objectives	704
Primary Control Plane Objective	706
Secondary Control Plane Objective	708
User Plane Objectives	715
Stateless UDP Traffic	717
Data Traffic	718
Voice Traffic	722
Video OTT Traffic	736
DNS Client Traffic	740
ICMP Client	743
Ping Traffic	744
Capture Replay	745
Predefined Applications Traffic	747

Control Plane Objective

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

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

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

About primary objectives

In the current 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](#)
- [Subscribers Per Second](#)

Active Subscribers

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

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

Subscribers Per Second

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

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

This can be viewed as a timeline:

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

Observations:

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

Example:

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

Such a test will give the following results.

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

Primary Control Plane Objective

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

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

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

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

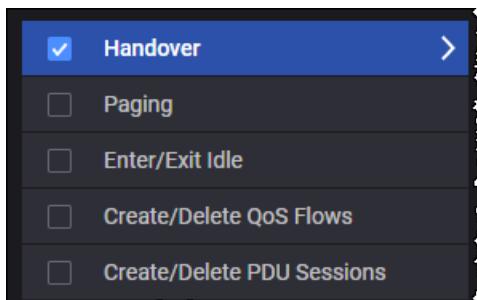
Secondary Control Plane Objective

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

IMPORTANT

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

In this example, only Handover has been selected:



Note that:

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

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

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

Handover

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

Handover configuration parameters

The following table describes these objective parameters.

Parameter	Description
<i>Handover:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which handovers are initiated, measured in procedures per second if Distributed over (s) is not modified.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Force N2	Enable this option to force N2 handover with direct forwarding instead of X2 / Xn

Parameter	Description
Handover	handover.
Mobility for State	<p>This option specifies in what state should the UE perform the handover objective. The following options can be selected from the drop-down list:</p> <ul style="list-style-type: none"> • Connected • Idle • Any <p>When Any is selected, the UE will execute the handover objective, regardless if the UE is in Connected or Idle state.</p>
Force UE State Before Returning to Parent Node	<p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • None - The UE will perform either Idle Mode Mobility or Connected Handover to parent RAN, depending on what state the UE is before executing the procedure. • Connected - The UE will perform Connected Handover from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in idle state before performing this mobility, the UE will first perform exit idle, and only after the UE is in connected state, will it initiate the connected handover to the parent RAN. • Idle - The UE will perform Idle Mode Mobility from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that if the UE was in connected state before performing this mobility, the UE will first perform enter idle, and only after the UE is in idle state, will it initiate the idle mode mobility to the parent RAN.
<i>Visited gNodeBs/eNodeBs : A list of the NG-RANs that UEs will visit during the test.</i>	
	Add next node to the list.
	Remove the selected node from the list.
Force UE State before Mobility	<p>The following options can be selected from the drop-down list:</p> <ul style="list-style-type: none"> • Connected • Idle • Any
Primary Node	Select the primary node from the drop-down list.
Secondary Node	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>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Suspend Traffic Interval (s)	The time (in seconds) to suspend traffic on the remote IP address.
Remote IP Address	<p>Set the remote IP address:</p> <ul style="list-style-type: none"> If the UPF is the DUT in the test topology, then set the <i>Remote IP Address</i> to the DN IP address. If the UPF is simulated in the test topology, then set the <i>Remote IP Address</i> to the N3 IP address of the UPF.

Notes:

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

Enter/Exit Idle

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

NOTE

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

The following table describes the objective parameters.

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

Create/Delete QoS Flows

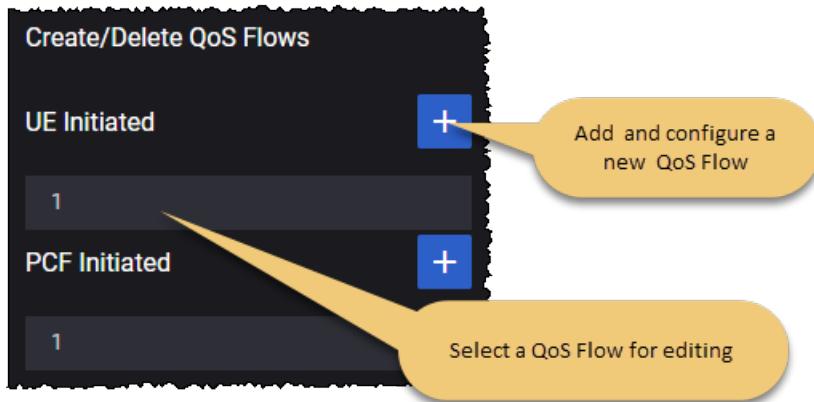
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured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

QoS flow options

There are two options for creating QoS flows:

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

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



Objective parameters

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

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

Parameter	Description
Interval	Interval between the triggering of creation and deletion of the QoS flow, in seconds.
DNN	Select the DNN value for the drop-down list. For example: dnn.keysight.com.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

Support for Network Initiated QoS Flow modification

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

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

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

Notes:

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

Create/Delete PDU Sessions

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

The following table describes the objective parameters.

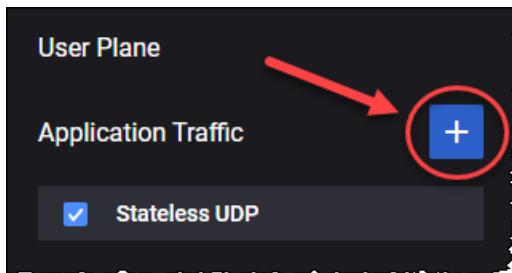
Parameter	Description
<i>Create/Delete PDU Sessions:</i>	
	Select the Add Objective button to add an instance of this objective.

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

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, Predefined Applications, ICMP Client and Ping.**

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 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

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

The following table describes the Stateless UDP parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Flow Type	This field is set to uplink and can not be modified since on the UE you can only configure the uplink flow.
Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
Destination IP Address	The destination IP address to place in the IP packet.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	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. <ul style="list-style-type: none"> • When this option is selected, traffic will flow from the start of the test until

Parameter	Description
	<p>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.</p> <ul style="list-style-type: none"> When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>

Data Traffic

The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Throughput . The other options are: Concurrent Connections and Connections Rate .
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to Concurrent Connections .
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to Concurrent Connections .
Connections Rate per Second	Set the value for connections rate per second. This parameter is available only when Objective type is set to Connections Rate .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.

Parameter	Description
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	<p>The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.</p>
IP Preference	<p>Select a value from the drop-down list: IPv4 or IPv6.</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 for a description of the configuration settings for these traffic flows.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> If Optimize Throughput (per UE) option is enabled: TCP, TLS, QUIC or UDP. If Optimize Throughput (per UE) option is disabled: TCP, TLS or UDP.
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> For TCP transport protocol: HTTP Get, HTTP Put, HTTP Post and FTP. For TLS transport protocol: HTTPS Get, HTTPS Put and HTTPS Post. For QUIC transport protocol: HTTP3 Get, HTTP3 Put and HTTP3 Post. For UDP transport protocol: UDP Bidirectional (a flow in which a UDP client communicates with a server over a bidirectional datagram socket) <div style="background-color: #f0f0f0; padding: 5px; margin-left: 20px;"> NOTE UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receives the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds. </div>
Port	The port used by the flow.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to UDP Bidirectional for more details.

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

Custom Parameters

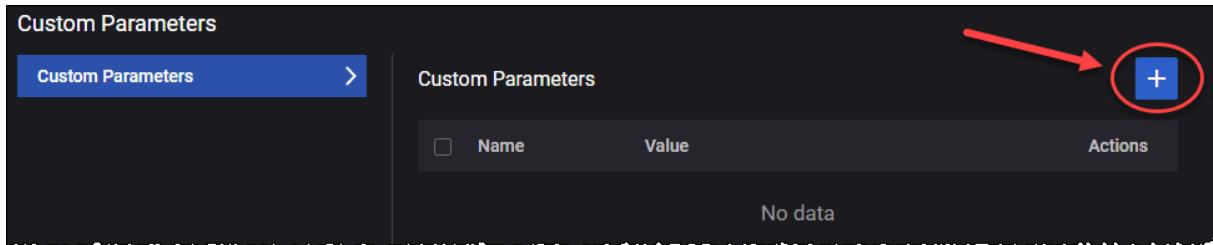
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

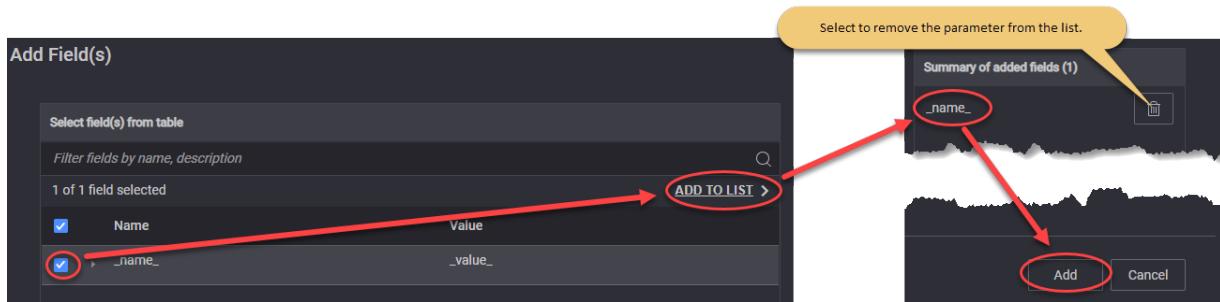
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Call Type	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.

Parameter	Description
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security • UDP - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	For more details about these settings, refer to Advanced SIP Settings .
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select this option in order to enable RTCP.
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
DNN ID	Select the DNN from the drop-down list.
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
Update IMSI and Source Phone with UE Range Identification Settings	Select this button in order to update IMSI and Source Phone with UE range identification settings.
IMSI	Read-only field, it displays the updated IMSI.
IMSI Phone Increment	The value by which the IMSI phone number is incremented.
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is

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

Media Settings

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

Parameter	Description
Media Duration (ms)	Length of time to play the media stream. You can accept the value provided by LoadCore or overwrite it with your own value.
QoS Flow ID for Voice	The QoS Flow ID for RTP traffic. Select the QoS Flows ID(s) from the drop-down list.
Enable video	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for video from the drop-down list. This parameter is available only when Enable video is selected.

Jitter Buffer Settings:

Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
--------------------	--

Audio Codecs

	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: <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

Parameter	Description
	<p>adopted as the standard speech codec by 3GPP.</p> <ul style="list-style-type: none"> • EVS - The EVS (Enhanced Voice Services) codec specified by 3GPP TS 26.445 compresses 20ms input blocks of audio samples. In addition to the EVS Primary mode, 3GPP TS 26.445 specifies that the codec implement the EVS AMR-WB IO mode for interoperability with AMR WB devices. • PCMU • PCMA • iLBC • G722 • G723 • G729 <p>The parameters of each audio codec are presented below.</p>
Video Codecs	<i>This section is available only when Enable video is selected</i>
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: H264 or H265 .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.
<i>Advanced Media Settings</i>	
Custom SDP	<i>Select this panel to open the custom SDP settings.</i>
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4 • NB Codecs IPv6 • AMR-WB IPv6 • Multimedia IPv4

Parameter	Description
QoE Settings	Select this panel to open the audio QoE settings.
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

AMR/AMR-WB

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

EVS

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

Parameter	Description
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.

Advanced SIP Settings

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

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

SIP Custom Headers

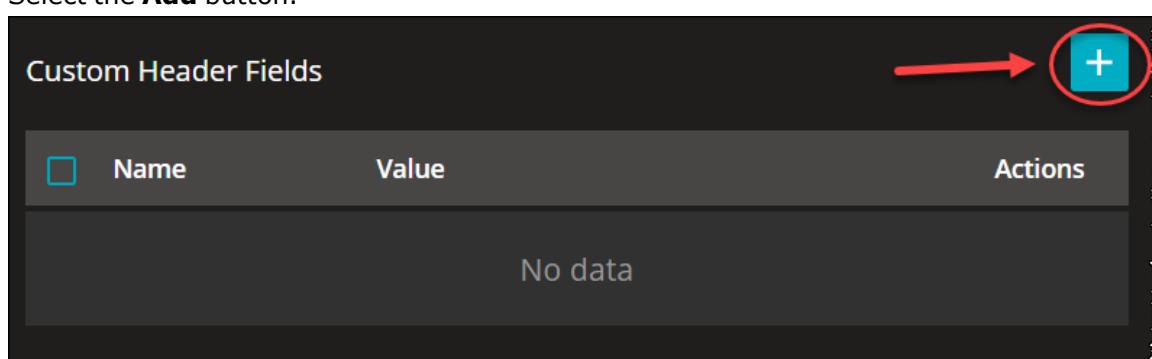
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE

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

For each message, you can:

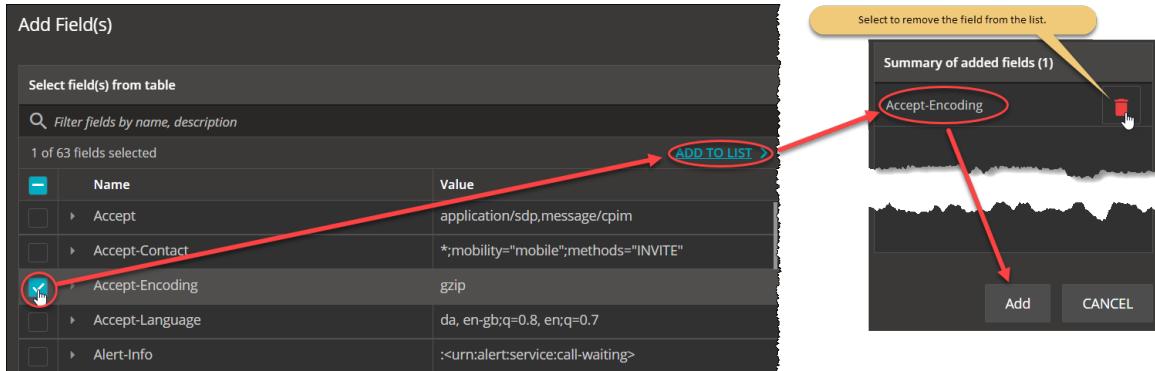
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
 - Select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom header are available:

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

Parameter	Description	Value
	IETF RFC 3310	
Call-Info	IETF RFC 3261	<http://www.example.com/alice/photo.jpg> ;purpose=icon
Content-Disposition	IETF RFC 3261	session
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:00 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC	3600

Parameter	Description	Value
	3261	
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC 4028	60
Organization	IETF RFC 3261	Keysight
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>

Parameter	Description	Value
	3327	
P-Called-Party-ID	IETF RFC 7315	sip:user1-business@example.com
P-Charging-Function-Addresses	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Charging-Vector	IETF RFC 7315	icid-value=1234bc9876e;icid-generated-at=192.0.6.8;orig- ioi=home1.net
P-Early-Media	IETF RFC 5009	supported
Permission-Missing	IETF RFC 5360	userC@example.com
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com", qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque ="", stale=False, algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice", realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",r esponse="245f23415f11432b3434341c022"
Proxy-	IETF	foo

Parameter	Description	Value
Require	RFC 3261	
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>, <sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org? Replaces=425928%40bobster.example.com.3%3Bto-tag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10

Parameter	Description	Value
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore

Parameter	Description	Value
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

SIP Authentication

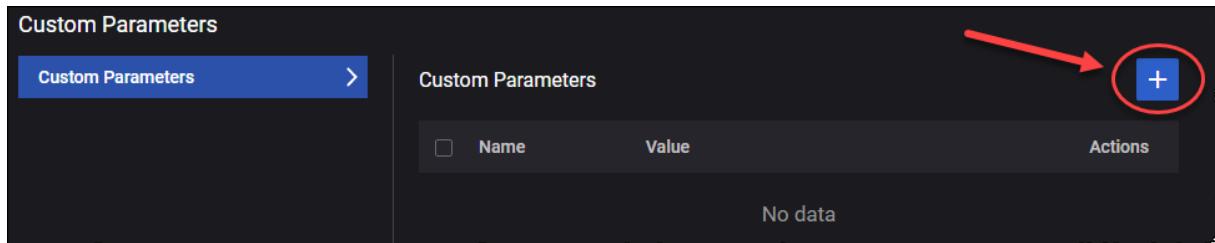
The parameters required for SIP authentication are presented in the table below.

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

Custom Parameters

You can add custom parameters as follows:

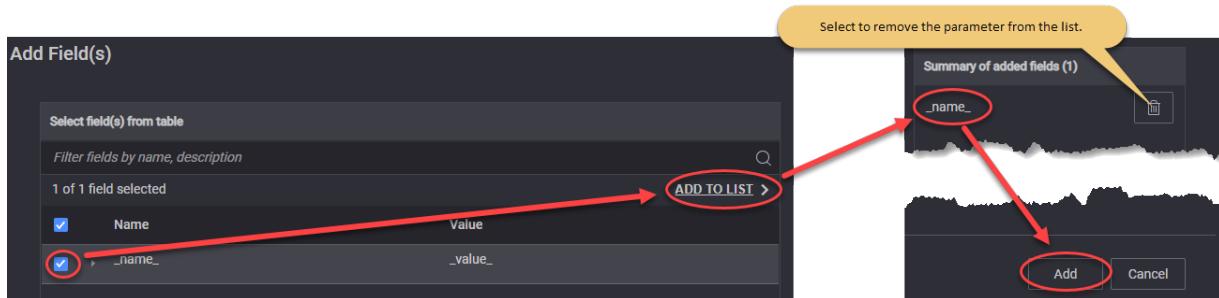
1. The Custom Parameters panel, select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom parameters are available:

Parameter	Description	Value
DelayBefore SIPInvite	Delay in milliseconds before sending SIP INVITE.	1000
DealyBeforeRTP	Delay in milliseconds before RTP session start.	0
DelayAfterRTP	Delay in milliseconds after RTP session end.	0
DeregisterLoop	Set the number of calls/loops before a SIP deregistration will be performed. Any SIP deregistration will be followed by a new SIP registration.	0
DelayBefore180	Delay in milliseconds before 180 Ringing message will be sent.	0
DelayBefore200INVITE	Delay in milliseconds before 200 OK message for INVITE will be sent.	0
debugIPSEC	Activate IPSEC debug. Please use debug only for a reduced number of simulated UEs.	0

Parameter	Description	Value
timeoutSIP	Global timeout in milliseconds for any SIP message. Default is set to standard 32000ms. Use this parameter to modify the default value.	32000
MaxActiveLimit	Set maximum allowed concurrent TCP connections per CPU Core. Default it is set to 8000. Please use this parameter to modify the default value.	8000

SIP 3GPP IPSEC

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

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

Video OTT Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Video OTT .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	Select the value from the drop-down list: Simulated Users or Throughput .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.

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 after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .
Advanced OTT	Select the Open Advanced OTT button to enable and configure Advanced OTT Settings .

Advanced OTT Settings

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

Parameter	Description
Application Traffic Flow	Each Application Traffic entry requires at least one Ott traffic flow definition, and can support multiple such definitions. <ul style="list-style-type: none"> To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings. To add another traffic flow, click the Add Flow button. 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 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

Parameter	Description
	playtime is used.
Play Duration (sec)	This field is available only if the Play Until End check box is not selected. It allows you to set a custom playtime.
Transport	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> • HTTP • HTTPS • HTTP/QUIC
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero).
Percentage	The percentage of Test Objective to execute this flow.
Quality Control	These settings are presented in the Quality Control pane.
Advanced Client settings	These settings are presented in the Advanced Client Settings pane.

Quality Control

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

Parameter	Description
<i>Jitter Buffer:</i>	
Initial Delay (s)	Set the number of seconds to wait before playback. The default value is 20.
Maximum Size (s)	Set the number of seconds to be buffered on the client side. The default value is 20.
MOS P.1203	Select an option from the drop-down list: Disabled or Mode 0 .
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> • Adaptive Bit Rate • Quality Predefined Levels • Lowest Quality • Highest Quality
Number of segments	This field is available and editable only when the Quality Control Mode is set to Adaptive Bit Rate .
<i>Play Profiles:</i> The following settings are available and editable only when the Quality Control Mode is set to Quality Predefined Levels .	

Parameter	Description
	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.
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

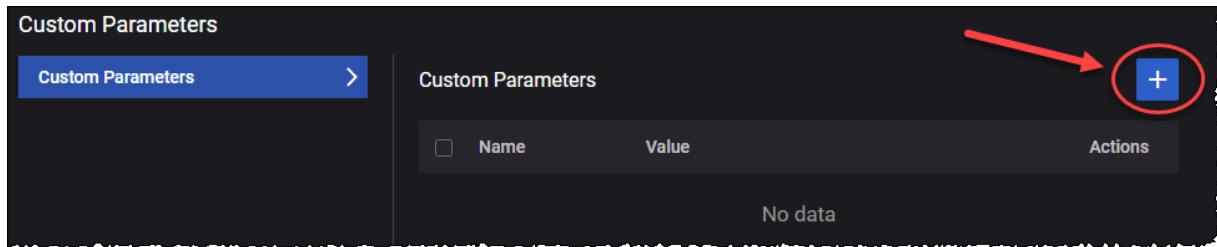
The parameters required for Advanced Client settings are presented in the table below.

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.
Enable DNS Query Per Connection	Select the check box to process only one DNS query per TCP connection.
Custom parameters	For more details, refer to Custom parameters .

Custom Parameters

You can add custom parameters as follows:

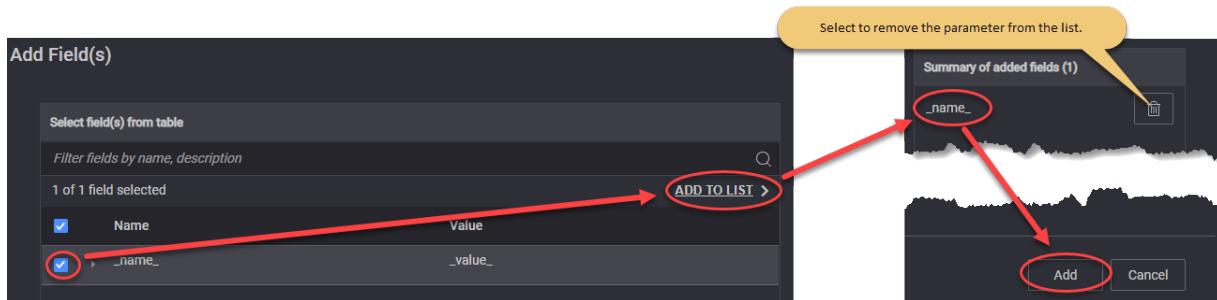
1. Select the **Open Custom Parameters** tile. The Custom Parameters panel opens.
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DNS Client Traffic

The following table describes the DNS Client Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to DNS Client .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Connection multiplier (per UE)	Set the value for the connection multiplier.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>

Parameter	Description
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
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 Flow for a description of the configuration settings for these traffic flows. Also, you can add custom parameters, based on your test configuration requirements.</p>

Flow

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

Parameter	Description
	Click the Delete Flow button to remove the flow from your configuration.
Type	By default, the type is set to DNS Client .
Port	The port used by the flow.
DNS Server IP	Set the DNS server IP address.
Number of DNS servers	Set the number of DNS servers.
Hostname	Set the hostname.
Query Type	Select the query type from the drop-down list. The available options are: <ul style="list-style-type: none"> • A • AAAA • CNAME • TXT • PTR • NS
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range Settings (DNNs Config).
QoS FlowID	Select a QoS Flow ID for this flow.

Custom Parameters

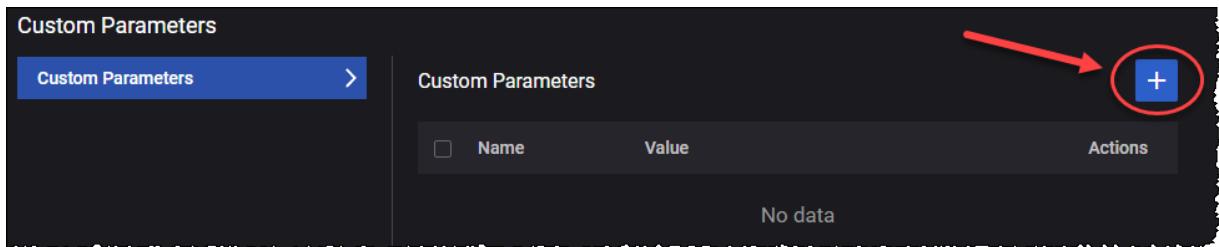
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

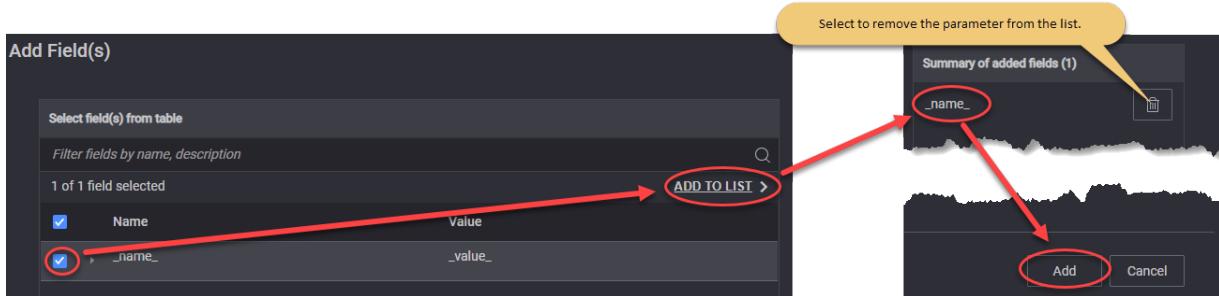
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



ICMP Client

The following table describes the ICMP Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to ICMP Client .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select the IP address preference: IPv4 or IPv6 .
Traffic Flow	Refer to Traffic Flow for a description of the configuration settings for these traffic flows.

Traffic Flow

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

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

Ping Traffic

This application traffic type emulates a PING client.

The following table describes the Ping Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
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.
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.
Count	Set the count value. Default value: 4.
Interval (ms)	Set the interval value. Default value: 1000.
Timeout (ms)	Set the timeout value. Default value: 4000.

Parameter	Description
DNN ID	Select the DNN for this flow. The DNNs are configured in the UE Range settings (DNNs Config).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: IPv4 or IPv6 .

Capture Replay

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

The following table describes the Capture Replay parameters.

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

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

The following table describes the Filter object parameters.

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

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

Predefined Applications Traffic

The following table describes the Predefined Flows Traffic parameters.

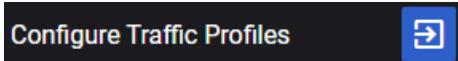
Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Predefined Applications .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> • Simulated Users • Throughput • Connections Per Second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

Parameter	Description
	unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
Configure Traffic Profiles	Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions. Refer to Traffic Profile for a description of the configuration settings for these traffic profiles.

Traffic Profile

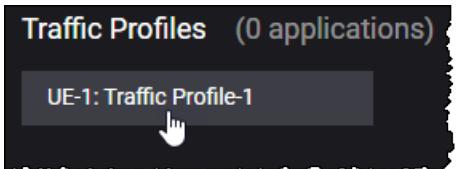
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

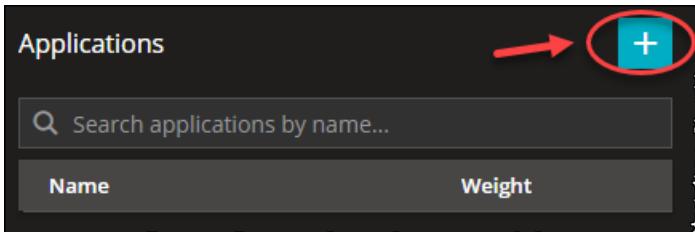
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

Applications

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

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



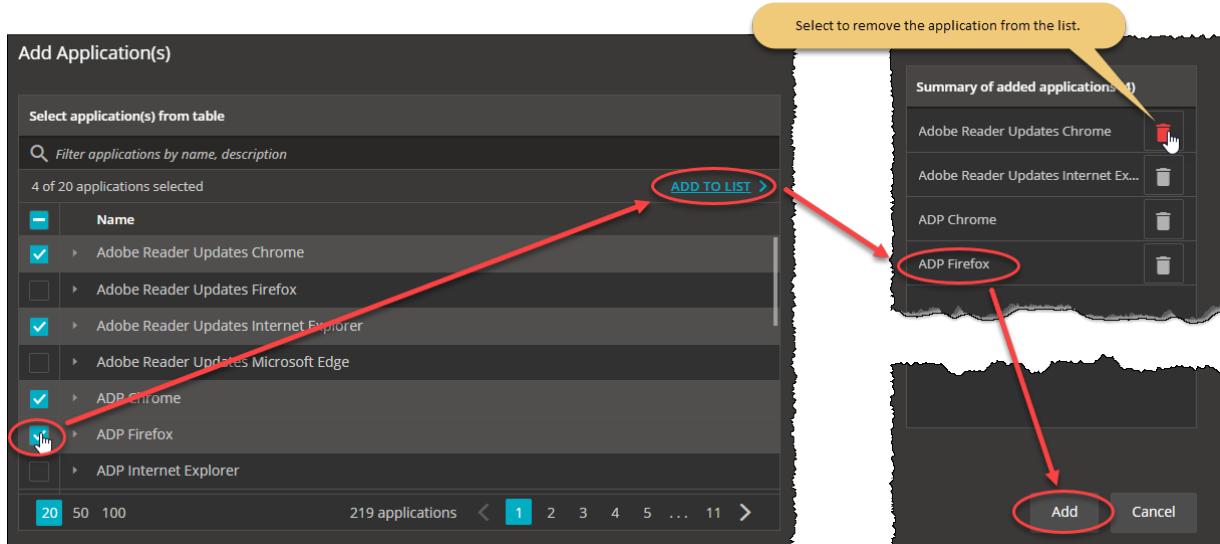
The Add Application(s) window opens.

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

NOTE

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

For example ...



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

For example ...

Applications		Edit	+
<input type="text"/> 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 CoreSim configuration interface. On the left, the 'Applications' section lists predefined applications with columns for Name and Weight. One application, 'Adobe Reader Updates Chrome 1', is selected and highlighted with a cursor icon. To the right, the 'Application Settings' section contains fields for Destination Hostname, DNN ID, and QoS Flow ID. Below this, the 'Application Actions' section shows a list of actions with columns for # and Name, including 'Check For Updates' and 'Download Updates'.

#	Name
1.	Check For Updates Client -> Server acroipm2.adobe.com
2.	Download Updates Client -> Server ardownload.adobe.com

Application Settings

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

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

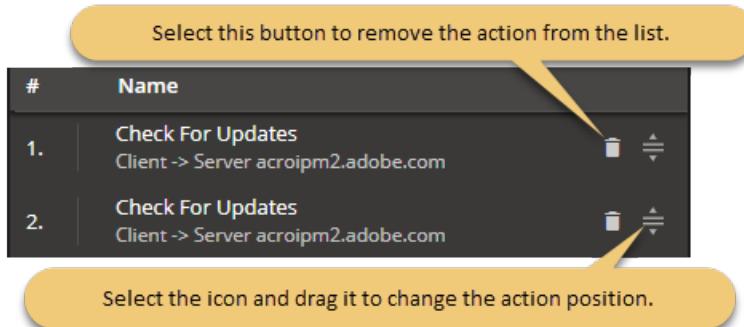
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

Application Actions

The Application Actions section lists the actions and action parameters available in 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:

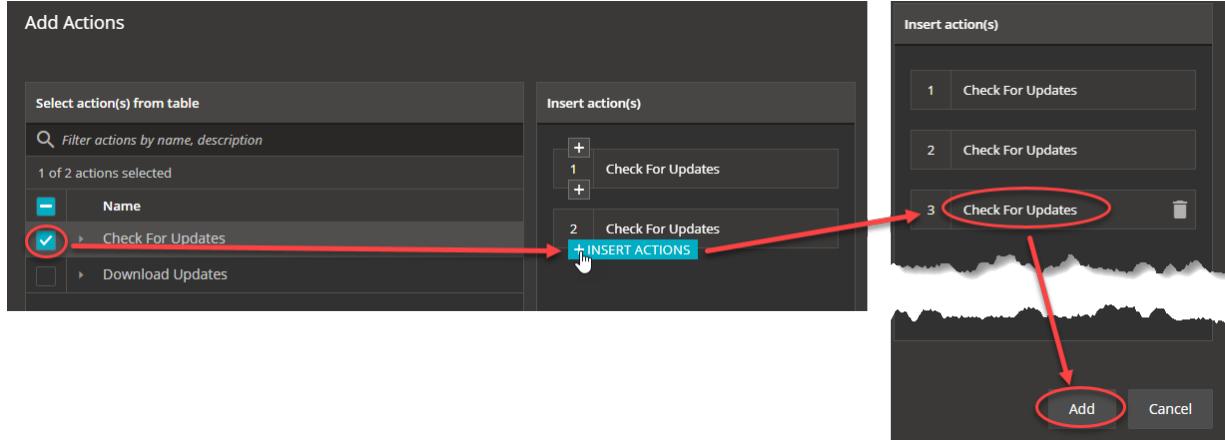
1. Use the icons available for each icon in order to remove it or to change its position in actions list.
For example ...



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 ...



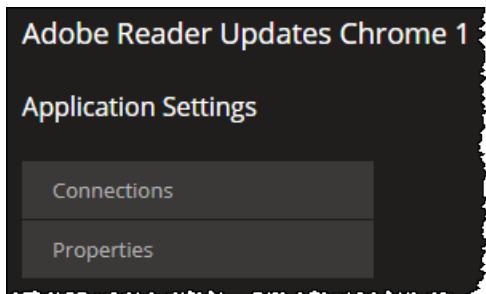
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

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.

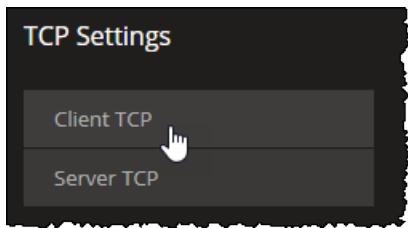
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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.



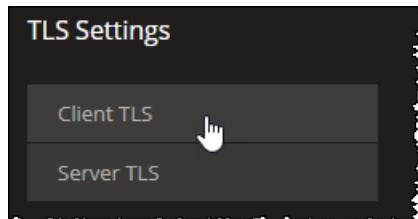
These parameters are configurable for both Client and Server settings, as presented in the following table.

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. <div style="margin-left: 20px;"> NOTE Enabling the TCP Timestamp option adds 12 bytes to the TCP header. This reduces the effective configured MSS. </div>

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.
SNI Enabled	<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.
Certificate file	<i>Select Upload to add your certificate file or Clear to remove it.</i>
Key file	<i>Select Upload to add your key file or Clear to remove it.</i>
Key file password	<i>Enter your key file password.</i>
DH file Traffic	<i>Select Upload to add your DH file or Clear to remove it.</i>

RTP Settings

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

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

DN configuration settings



Data Networks (DN) represents one of the entities in the 5G core network architecture. DN interfaces 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:

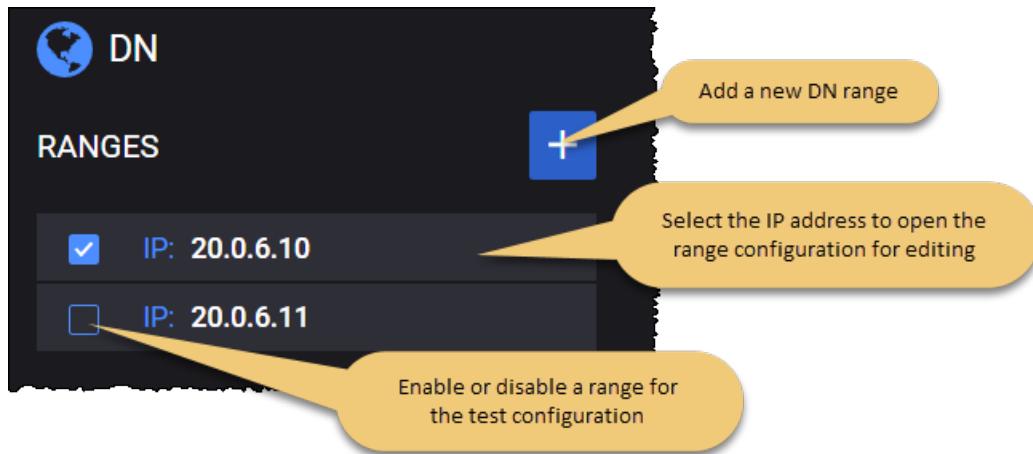
DN Ranges panel	758
DN Range panel	759
DN N6 interface settings	760
DN routes settings	761
DN User Plane	762
DN Stateless UDP Traffic	763
DN Data Traffic	764
DN Voice Traffic	766
DN Video OTT Traffic	776
DN DNS Server Traffic	779
DN Predefined Applications Traffic	781
DN Capture Replay	782

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 **Routes Settings** to configure the route to an UE or custom range.
- Select **User Plane** to configure the traffic generators.

DN range controls and settings

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

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

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

Setting	Description
User Plane	These settings are described in DN User Plane .

DN N6 interface settings

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

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

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.
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. Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.

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

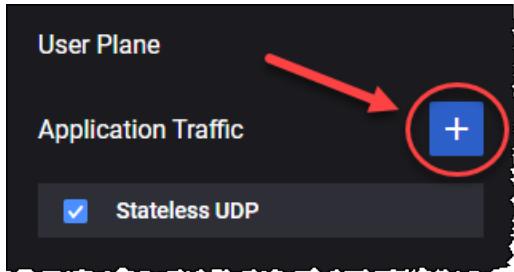
DN routes settings

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

Settings	Description
<i>Routes Config:</i>	
	Select this button to add a new route to a specific UE range or a custom one.
<i>UE Routes Config:</i>	
	Select this button to remove the route.
Route Type	Select the route type from the drop-down list. Available options: UE or Custom .
UE Range MSIN	Select the MSIN of the UE range from the drop-down list.
Peer UPF	Select the UPF node connected to DN over the N6 interface from the drop-down list.
Gateway Address	The IP address assigned as gateway address.
DNN(s)	<p>Select the DNNs from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> • All: Select this item to choose all of the available DNNs that are configured for the UE. • specific DNNs: Select one or more of the individual DNNs from the list.
Destination Subnet Address	<p>Set the destination subnet address. This parameter is available only when the route type is set to Custom.</p>
IP Prefix Length	<p>The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address. This parameter is available only when the route type is set to Custom.</p>

DN User Plane

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



NOTE

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

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

DN Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Stateless UDP .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Flow Type	This field is set to dowlink and can not be modified since on the DN you can only configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Destination UDP Port Start	The start destination port number to place in the UDP header.
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.
Destination UE Range	Select the destination UE range from the drop-down list.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to DNN configuration settings .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to QoS Flow configuration settings .
Fallback to Default Flow	<p>This option supports use cases in which it is desirable for user traffic to use the default QoS flow if the requested dedicated flow is not available.</p> <ul style="list-style-type: none"> When this option is selected, traffic will flow from the start of the test until the end. If the dedicated flow or bearer is not yet activated, it will fall back to the default flow. Once the dedicated bearer becomes active the traffic will move to that flow. If the dedicated bearer is deleted, the traffic will move back to the default flow.

Parameter	Description
	<ul style="list-style-type: none"> When this option is not selected, traffic will not flow until the designated QoS flow is activated (the flow selected in the <i>QoS Flow/Bearer ID</i> field). <p>This option is useful in a test in which you are using more than one traffic type. For example, you may want HTTP traffic to be running throughout the duration of the test while voice traffic is running only when a default flow is activated for it.</p>

DN Data Traffic

The following table describes the DN Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Data .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Application Servers	<p>Each Application Traffic entry requires an application server definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"> To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings. To add another application server, click the Add Server button. LoadCore will open the Server panel where you will select the server type and configure the server settings. <p>Refer to Server (below) for a description of the configuration settings required by the application server.</p> <p>Also, you can add custom parameters, based on your test configuration requirements.</p>

Server

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

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

Custom Parameters

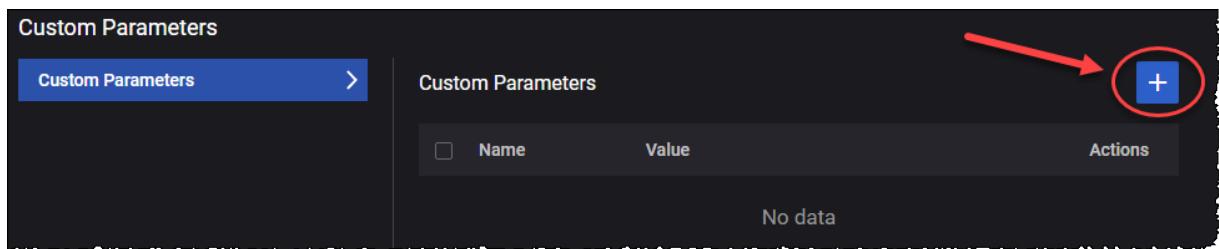
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

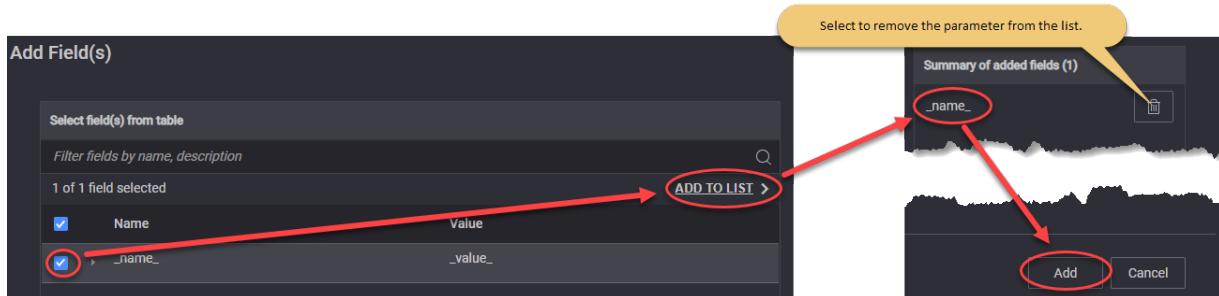
2. Select the **Add** button.



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 ...



DN Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to Voice .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	By default, this parameter is set to Simulated Users and cannot be changed.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Call Type	Select the type of call from the drop-down list.
Dial Plan:	<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

Parameter	Description
	overwrite it with your own value.
Transport Protocol	Select the transport protocol. The available options are: <ul style="list-style-type: none"> • TCP - Transmission Control Protocol • TLS - Transport Layer Security • UDP - User Datagram Protocol
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	For more details about these settings, refer to Advanced SIP Settings .
<i>RTP Settings</i>	
Local Port	Set the local port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Local Port Increment	The value by which the local port number is incremented.
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select the check box in order to enable this option.
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
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.

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.

Parameter	Description
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	Select the audio codec from the drop-down list. The available options are: <ul style="list-style-type: none"> • AMR - The Adaptive Multi-Rate (AMR) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • AMR-WB - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP. • EVS - The EVS (Enhanced Voice Services) codec specified by 3GPP TS 26.445 compresses 20ms input blocks of audio samples. In addition to the EVS Primary mode, 3GPP TS 26.445 specifies that the codec implement the EVS AMR-WB IO mode for interoperability with AMR WB devices. • PCMU • PCMA • iLBC • G722 • G723 • G729 The parameters of each audio codec are presented below.
<i>Advanced Media Settings</i>	
Custom SDP	Select this panel to open the custom SDP settings.
Use Custom SPD	Select the check box to use the custom SDP.
Custom SDP Template	Select the template from the drop-down list: <ul style="list-style-type: none"> • None • EVS/AMR IPv4

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

AMR/AMR-WB

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

EVS

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

Parameter	Description
	<ul style="list-style-type: none"> 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.

Advanced SIP Settings

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

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

SIP Custom Headers

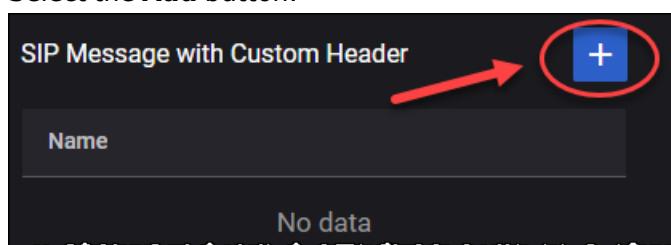
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

NOTE

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

For each message, you can:

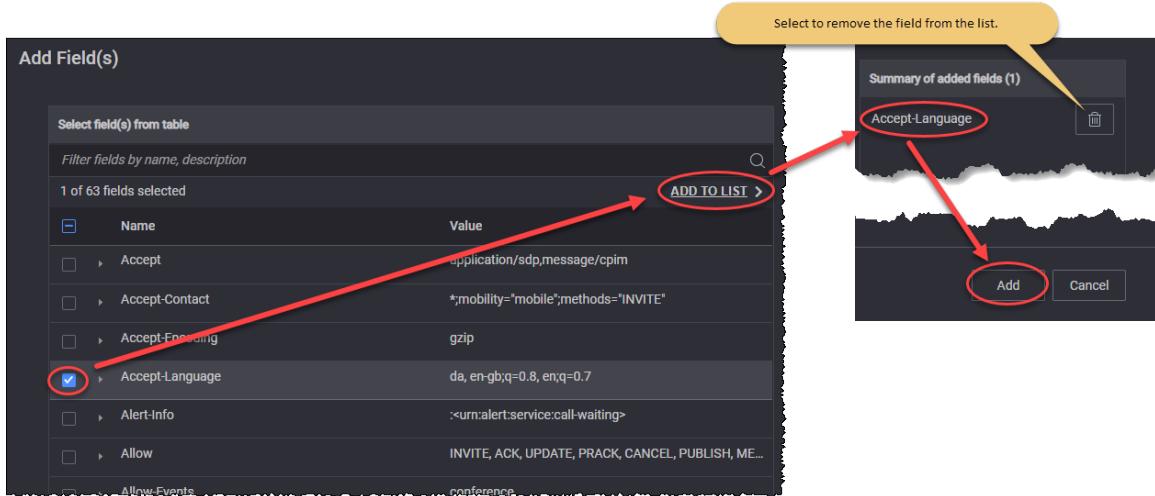
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
 - Select the **Add** button.



The Add Field(s) opens.

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

For example ...



The following custom header are available:

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

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

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

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

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

SIP Authentication

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

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

Parameter	Description
UPDATE	Select this button to update with UE range security settings.
K	The K (Subscriber Authentication Key) value used for authentication of the UEs in this range. The key is a string with a maximum length of 34 characters. You can accept the value generated by 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.

DN Video OTT Traffic

The following table describes the Video OTT Traffic parameters.

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

Parameter	Description
	Select this button to add an OTT server to your test configuration.
	Select this button to remove the OTT server from the test configuration.
Server Name	Set the server name. Each server is identified by a unique name. You can accept the value provided by 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 • HTTP/QUIC
Port	Set the port number. 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.
Streams	Refer to Streams (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Streams

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



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

Parameter	Description
	Select this button to add a stream to your test configuration.
	Select this button to remove the stream from the test configuration.
Stream Name	Set the stream name. Each server is identified by a unique name. You can accept the value provided by 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

Parameter	Description
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.</i>
	Select this button to add a quality level to your test configuration.
	Select this button to remove the quality level from the test configuration.
Bitrate (kbps)	Set the value of the bitrate.
Resolution	Select the resolution from the drop-down list. Available options: QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K .
Frames per second	Set the number of frames per second.

Custom Parameters

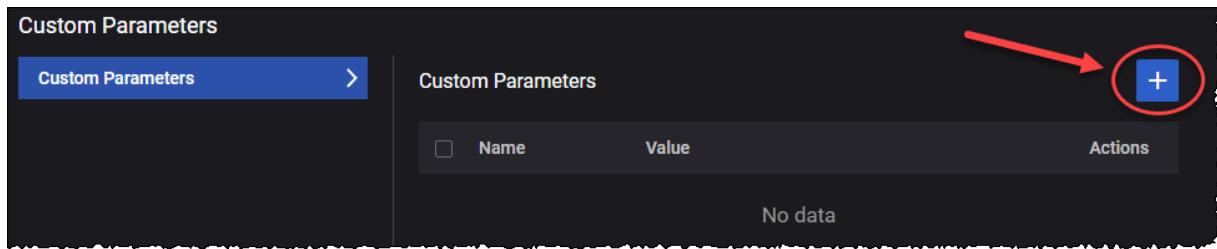
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

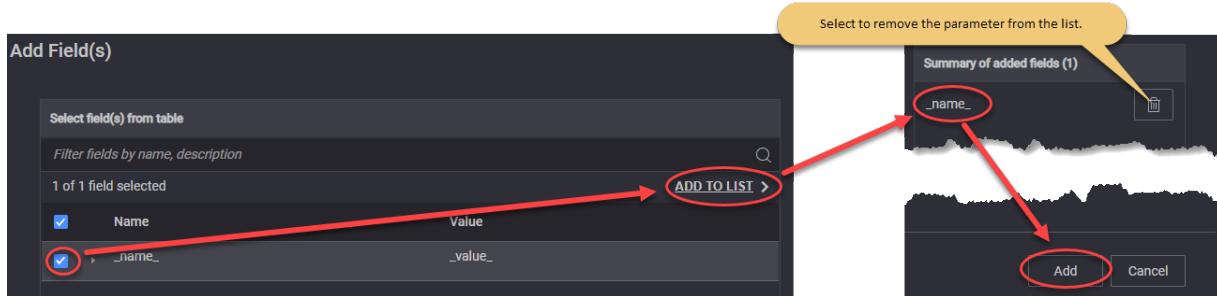
2. Select the **Add** button.



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 ...



DN DNS Server Traffic

The following table describes the DNS Server Traffic parameters.

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

Parameter	Description
	Select this button to remove the DNS server from the test configuration.
Type	Select the type from the available options.
Port	Set the port number. You can accept the 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.
Zone Manager	Refer to Zone Manager for descriptions of the DNS server zones settings.
Custom Parameters	You can add custom parameters , based on your test configuration requirements.

Zone Manager

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



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

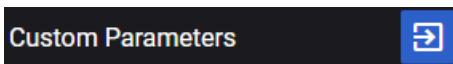
Parameter	Description
	Select this button to add a zone to your test configuration.
	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by LoadCore or overwrite it with your own value.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

Parameter	Description
	<ul style="list-style-type: none"> • CNAME • TXT • PTR • NS
Hostname	Set the hostname.
Address	Provide the address.

Custom Parameters

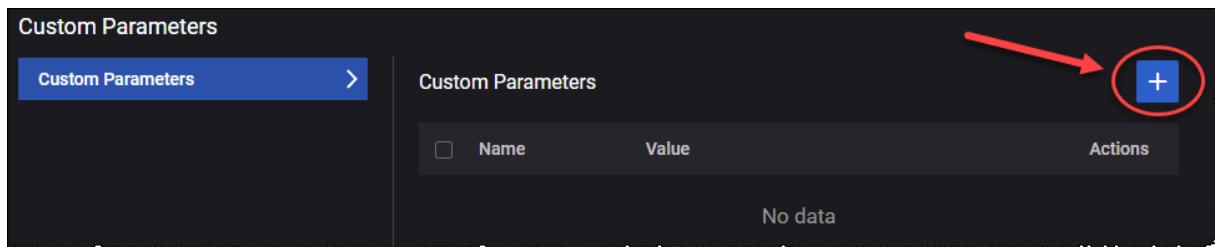
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

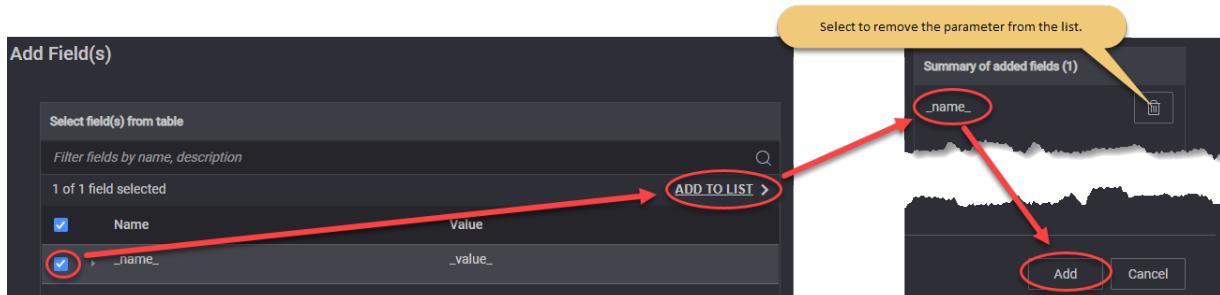
2. Select the **Add** button.



The Add Field(s) opens.

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

For example ...



DN Predefined Applications Traffic

The following table describes the Predefined Applications parameters.

Parameter	Description
Application	Select the type of traffic you want to generate. In this case, this parameter must

Parameter	Description
Type	be set to Predefined Applications .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Predefined Traffic Profiles	Select the traffic profile from the available options.

DN Capture Replay

The following table describes the Capture Replay parameters.

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

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

The following table describes the Filter object parameters.

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

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

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 **785**

Media Function Range panel **786**

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 select **CSCF Settings** to configure the node and connectivity settings for the CSCF range.:

CSCF range controls and settings

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

Setting	Description
<i>P-CSCF Node Settings</i>	
Domain	Set the domain name.
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Authentication Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: keysight.com .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: Digest , AKAv2 or AKAv1 .

Setting	Description
Algorithm	Select the algorithm from the drop-down list. Available options: MD5 , MD5-Sess , SHA256 or SHA256-Sess .
Quality of Protection	Select an option from the drop-down list: auth or auth-init .
<i>Connectivity Settings</i>	
IP Address	Set the IP address.

Media Function Range panel

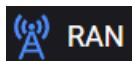
When you select a Media Function's IP address from the **Media Function Ranges** panel, LoadCore opens the **Range** panel, from which you can configure the connectivity settings for the Media Function range.

Media Function range controls and settings

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

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

RAN 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.

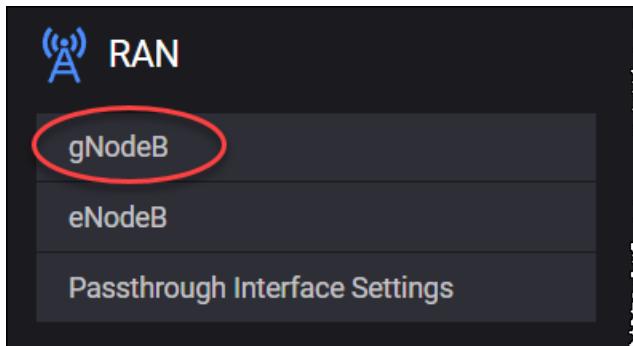
The configuration settings are described in the topics listed below.

Topics:

gNodeB	787
gNodeB Ranges panel	788
gNodeB Range settings	792
gNodeB node settings	793
gNodeB NSSAI settings	795
gNodeB N2 interface settings	796
gNodeB N3 interface settings	800
eNodeB	804
eNodeB Ranges panel	804
eNodeB Range Settings	808
eNodeB Node Settings	809
S1-U Interface Settings	809
S1-MME Interface Settings	811
Passthrough interface settings	812

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	788
gNodeB Range settings	792
gNodeB node settings	793
gNodeB NSSAI settings	795
gNodeB N2 interface settings	796
gNodeB N3 interface settings	800

gNodeB Ranges panel

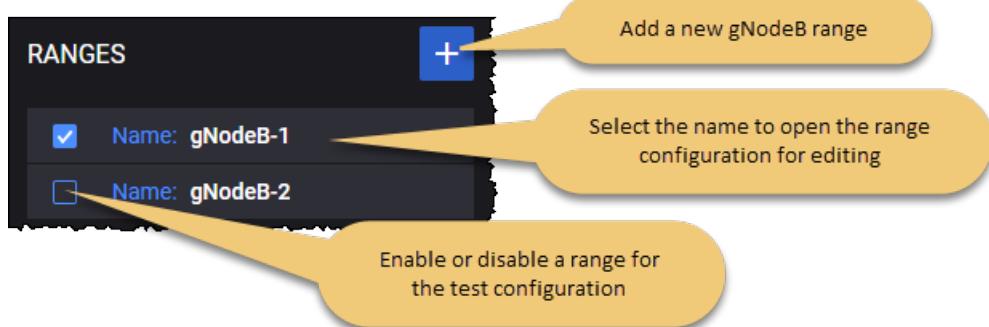
The **gNodeB Ranges** panel opens when you select **gNodeB** from the RAN pane. It consists of two main section: Ranges and Ranges Connectivity.

Ranges

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

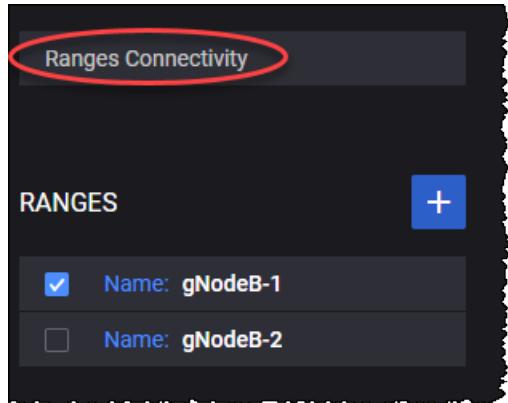
- Add a new gNodeB range to your test configuration.
- Open a gNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

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.

Ranges Connectivity		Matrix main check-box			
RANGES		gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4
<input checked="" type="checkbox"/> Name: gNodeB-1	<input type="button" value="+"/>	<input type="checkbox"/>	<input type="checkbox"/> Xn link check-box		
<input checked="" type="checkbox"/> Name: gNodeB-2		<input type="checkbox"/>			
<input checked="" type="checkbox"/> Name: gNodeB-3		<input type="checkbox"/>	<input type="checkbox"/>		
<input checked="" type="checkbox"/> Name: 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.

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

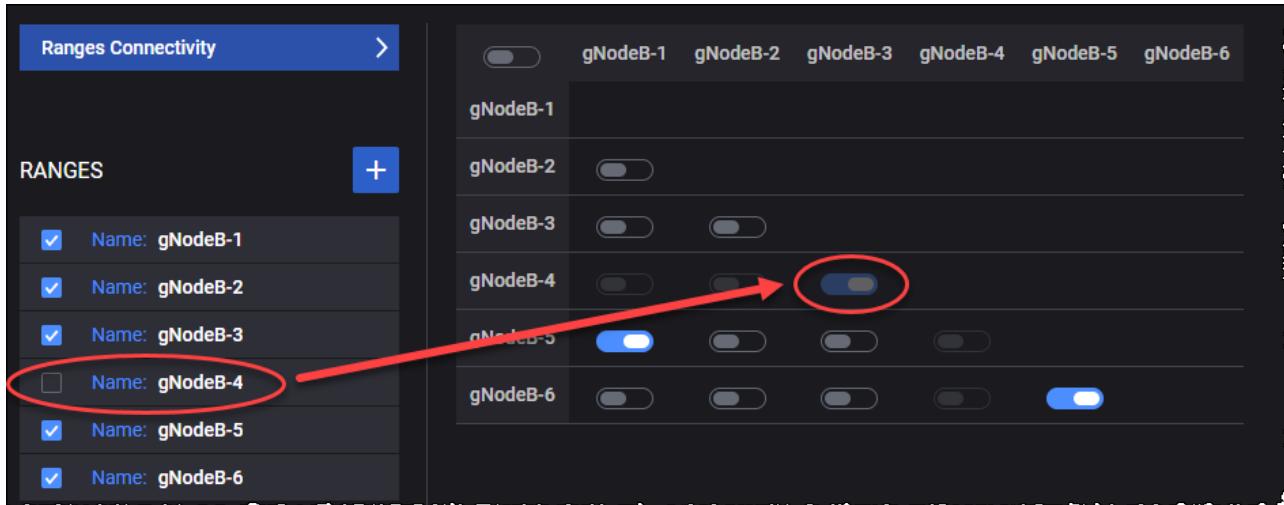


If there was an Xn link between two gNodeB ranges and now one of them is disabled, the check-box will become greyed out and cannot be unselected.

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

For example ...

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



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

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

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

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

Even the Xn link check-boxes for disabled gNodeB ranges are selected since the Xn links for disabled gNodeB ranges are not sent to the traffic agent. This way, when the disabled gNodeB range is

enabled, you will not have to manually select the Xn link check-boxes for that particular gNodeB range.

gNodeB Range settings

You add and select gNodeB ranges from the gNodeB Ranges panel. When you select the name of an gNodeB range, 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 describe in gNodeB node settings .
NSSAI	Each gNodeB range requires the configuration of at least one NSSAI, and may specify multiple NSSAIs. These settings are described in gNodeB NSSAI settings .
N2 Interface Settings	Each gNodeB range requires the configuration of N2 interface settings, through which a gNodeB instance enables connectivity and interaction with the AMF component in the 5G network. These settings are described in gNodeB N2 interface settings .
N3 Interface Settings	Each gNodeB range requires the configuration of N3 interface settings, through which a gNodeB instance enables connectivity and interaction with the UPF component in the 5G network. These settings are described in gNodeB N3 interface settings .

gNodeB node settings

Each gNodeB range includes a set of Node Settings.

Node Settings

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

Setting	Description
Name	Multiple gNodeB instances may be deployed in the 5G network. Each gNodeB instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by 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.
gNodeB ID Length	The number of bits from the Cell Identity to use as the gNodeB ID.
Cell ID	The NR Cell Identity (NCI) for the cell associated with this node range.
Connection Timeout (ms)	The S1AP connection timeout.
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.

EPS Fallback Settings

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

The following parameters are required to configure the EPS fallback:

Setting	Description
Enable EPS	Select the check box to enable this option.

Setting	Description
Fallback	
5QI	<p>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 101 panel in the Global Settings.)</p> <p>When a request is received for this 5QI to create a dedicated QoS flow, the RAN will reject the request, which will trigger the EPS fallback procedure.</p>
Associated ENB	Select the eNodeB used for handover.
Secondary Node	<p>Select the secondary node from the drop-down list.</p> <p>This option is used for EPS fallback to an eNodeB associated to a gNodeB using Option 3x.</p>
EPS Fallback Mobility	<p>Type of mobility to EPS during EPS fallback.</p> <p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • Handover to 4G • Inter-System Redirection to 4G
EPS Fallback Return Mobility	<p>Type of mobility that occurs after the deletion of the dedicated bearer that triggered EPS fallback.</p> <p>Select an option from the drop down list:</p> <ul style="list-style-type: none"> • None - After the dedicated bearer is deleted in 4G, the UE will not initiate any procedure. • Connected Mode Handover to 5G (default value) - After the dedicated bearer is deleted in 4G, the UE will initiate a 4G to 5G Connected Mode Handover. • Idle Mode Mobility to 5G - After the dedicated bearer is deleted in 4G, the UE will perform an Enter Idle procedure in 4G, followed by a 4G to 5G iRAT Idle Mode Mobility.

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

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

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

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

Setting	Description
Public Warning System	Select the check box to enable this option.

Setting	Description
PWS Restart Timer (s)	Duration in seconds after which PWS Restart Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.3 PWS Restart Indication</i> .
PWS Failure Timer (s)	Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. 0 indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.4 PWS Failure Indication</i> .

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, NASSAI 2,...NASSAI X) as required to meet your test objectives.

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

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

Setting	Description
NSSAI:	
	Select the Add NSSAI button to add a new NSSAI to your test configuration.
NSSAI settings:	
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.
SST	The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:

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

gNodeB N2 interface settings

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

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

By default, the N2 interface check box is enabled.

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

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

N2 Interface Settings

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

Settings	Description
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum Retransmission Timeout (ms)	Set the maximum retransmission timeout value, in milliseconds.
Initial Retransmission Timeout (ms)	Set the initial retransmission timeout value, in milliseconds.
Maximum Retransmission per Association	Set the maximum retransmissions value per association.
Maximum Retransmission per Path	Set the maximum retransmissions value per path.
Heartbeat Interval (ms)	Set the heartbeat interval value, in milliseconds.
SACK Delay (ms)	Set the delayed selective ACK timeout value.
SACK Frequency	Set the delayed selective ACK frequency value.

Connectivity Settings

Settings	Description
<i>IPSec: Select the check box to enable IPsec option.</i>	
Peer SEG	Select the peer SEG range from the drop-down list.
Destination Port	By default, the destination port is set to 500 and cannot be changed.
Source Port	Set the source port number.
Inner IP Type	Select the IP type: IPv4 or IPv6 .
<i>Authentication</i>	
Authentication	By default, the authentication method is set to Certificates and cannot be

Settings	Description
Method	changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	<p>It allows you to upload an archive that contains the certificates and keys for the gNodeB range, using the Upload button. To remove the archive , select the Clear button.</p> <p>The .key and .crt files need to have the same name before extensions.</p>
Use Same Certificates and Private Key For All Tunnels	By default, this option is disabled. Select the toggle button to enable it.
<i>IKE Phase 1</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. • If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	<p>Select an option from the drop-down list.</p> <p>Default value: prime256v1(19). Available options: prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32).</p>
PRF Algorithm	<p>Select an option from the drop-down list.</p> <p>Default value: HMAC-SHA256. Available options: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512.</p>
<i>IKE Phase 2</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-</p>

Settings	Description
	192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list.</p> <p>Default value: ID_DER ASN1 DN. Available options: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER ASN1 DN, ID_KEY_ID.</p>
Local Identification Value	<p>Set the value for this parameter.</p> <p>This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR.</p>
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
DPD Interval (s)	<p>Set a value for this parameter.</p> <p>Default value: 0 (disabled).</p>
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.

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).
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	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. Select the check-box to make this option available, and, then, select the Inner VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID..

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
<i>IPSec: Select the check box to enable IPsec option.</i>	
Use N2 IPsec Tunnel	<p>This option is available only if IPsec check box is selected on the N2 interface. When this option is selected, the IPSec configuration from the N2 interface will be used for the N3 interface. Otherwise, N3 IPsec configuration is required.</p>
Peer SEG	Select the peer SEG range from the drop-down list.
Destination Port	By default, the destination port is set to 500 and cannot be changed.
Source Port	Set the source port number.
Inner IP Type	Select the IP type: IPv4 or IPv6 .
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to Certificates and cannot be changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	<p>It allows you to upload an archive that contains the certificates and keys for the gNodeB range, using the Upload button. To remove the archive , select the Clear button.</p> <p>The .key and .crt files need to have the same name before extensions.</p>
Use Same Certificates and Private Key For All Tunnels	By default, this option is disabled. Select the toggle button to enable it.
<i>IKE Phase 1</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> • When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE.

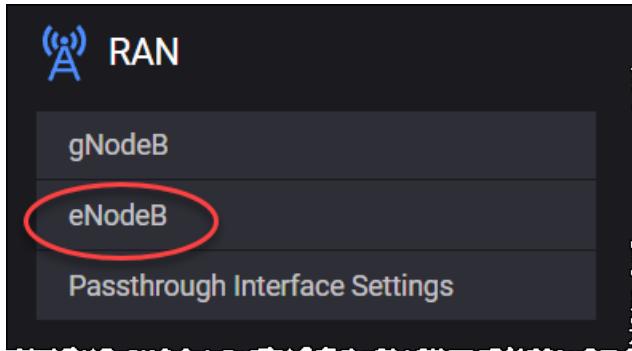
Connectivity Settings	Description
	<ul style="list-style-type: none"> If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
DH Group	<p>Select an option from the drop-down list.</p> <p>Default value: prime256v1(19). Available options: prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32).</p>
PRF Algorithm	<p>Select an option from the drop-down list.</p> <p>Default value: HMAC-SHA256. Available options: HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512.</p>
<i>IKE Phase 2</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: AES-128-GCM-16. Available options: AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: NONE. Available options: NONE, HMAC-MD5-96, HMAC-SHA1-96, HMAC-MD5-128, HMAC-SHA1-160, HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> When <i>Encryption Algorithm</i> is set to one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the only available <i>Hash Algorithm</i> is NONE. If Encryption Algorithm is set to a value other than one of AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16, the NONE hash algorithm is not available.
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list.</p> <p>Default value: ID_DER ASN1 DN. Available options: ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER ASN1 DN, ID_KEY_ID.</p>
Local Identification Value	<p>Set the value for this parameter.</p> <p>This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR.</p>
<i>Timers</i>	

Connectivity Settings	Description
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: 0 (disabled).
<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.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>

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

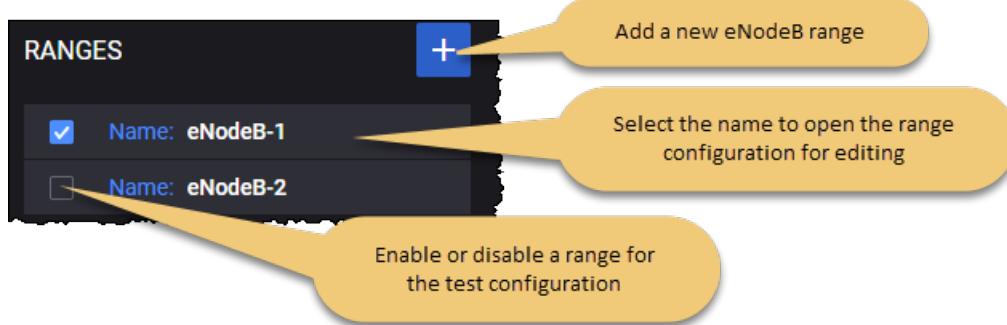
eNodeB Ranges panel	804
eNodeB Range Settings	808
eNodeB Node Settings	809
S1-U Interface Settings	809
S1-MME Interface Settings	811

eNodeB Ranges panel

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

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

For example ...



Ranges Connectivity

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

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

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

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

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

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

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

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

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

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

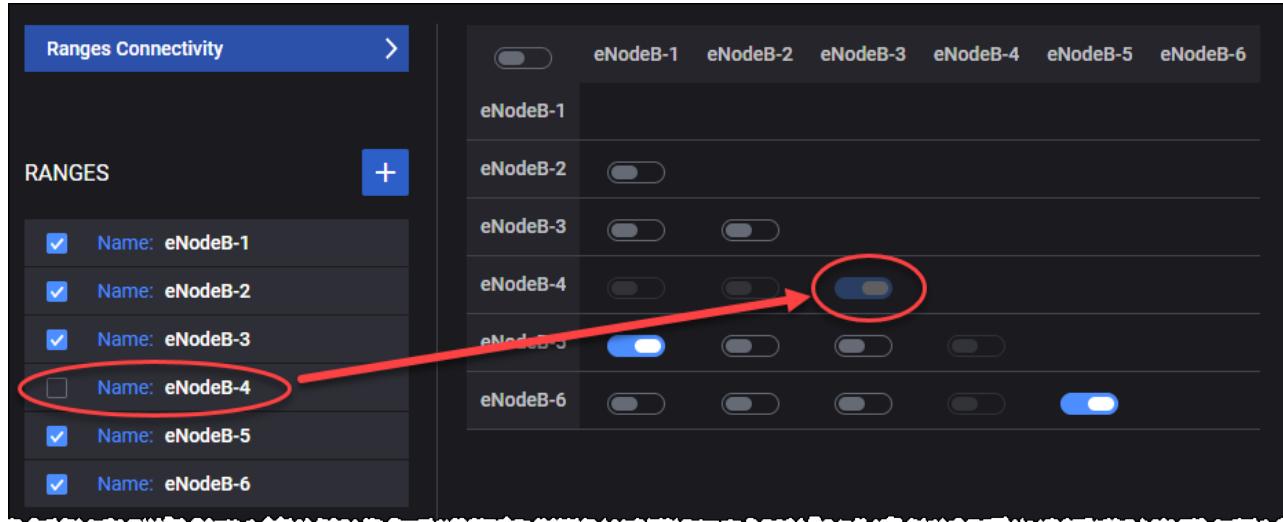
	eNodeB-1	eNodeB-2	eNodeB-3	eNodeB-4	eNodeB-5	eNodeB-6
eNodeB-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input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

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

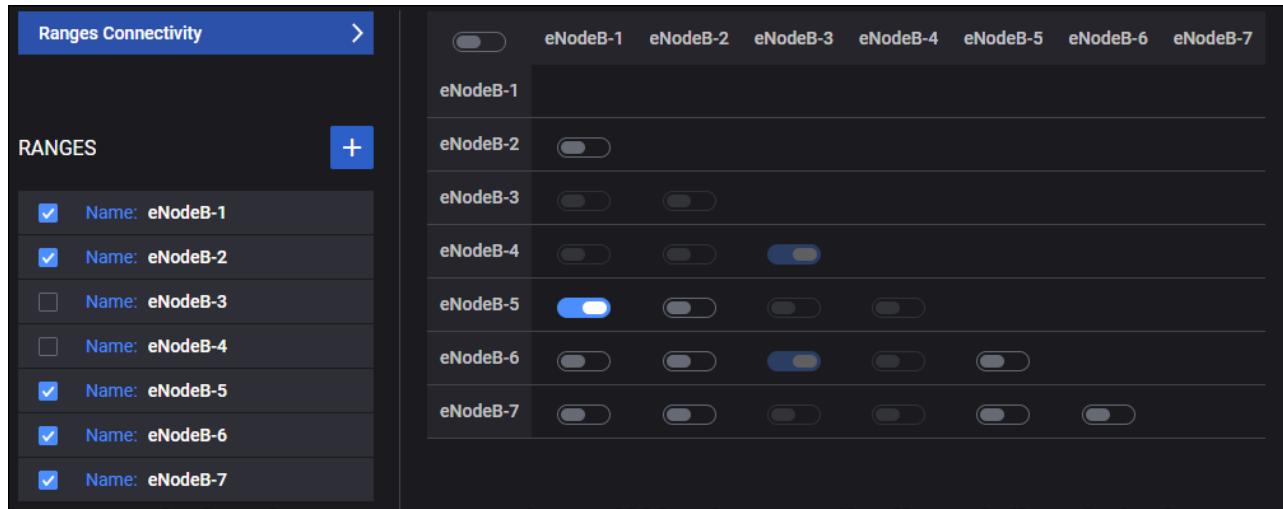
NOTE None of the X2 links that are part of disabled eNodeB ranges are sent to the traffic agent.

For example ...

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



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



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

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

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

Ranges Connectivity >		eNodeB-1	eNodeB-2	eNodeB-3	eNodeB-4	eNodeB-5	eNodeB-6	eNodeB-7
RANGES +		eNodeB-1						
		eNodeB-2	<input checked="" type="checkbox"/>					
		eNodeB-3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>				
		eNodeB-4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>			
		eNodeB-5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
		eNodeB-6	<input checked="" type="checkbox"/>					
		eNodeB-7	<input checked="" type="checkbox"/>					

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

eNodeB Range Settings

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

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

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

eNodeB Node Settings

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

Setting	Description
Name	The name of this eNodeB range. Multiple eNodeB instances (ranges) may be deployed in the test network. Each eNodeB instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by 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.
eNodeB ID Length	The number of bits to use for the eNodeB ID. It can have either 20 bits or 28 bits.
Cell ID	The Cell Identifier for this eNodeB range. The Cell Identifier is an 8-bit value that identifies a cell within the eNodeB. The same Cell Identifier is used for each eNodeB defined in a range.
Connection Timeout (ms)	The S1AP connection timeout.
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.

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

Connectivity Settings	Description
	<i>Inner VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

S1-MME Interface Settings

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

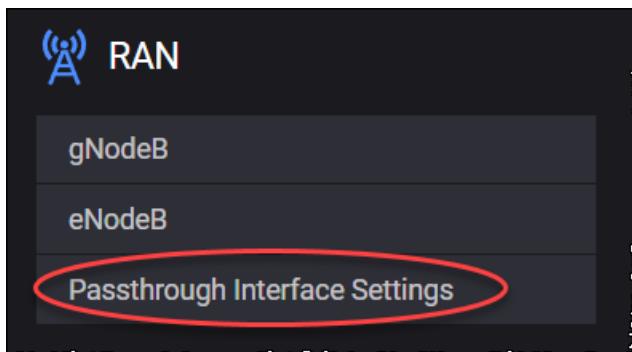
In order to run a test using the S1 interface, the eNodeB range must be enabled and configured with a Peer MME.

S1 Interface Settings	Description
Peer MME	Select the name of the peer MME node from the drop-down list.
SCTP Source port	The source SCTP port for control plane messages (NG-AP signaling messages). Each SCTP endpoint provides the other endpoint with a list of transport addresses 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.
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface. 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.

S1 Interface Settings	Description
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
Stack Type	Select the stack type from the drop-dpwn list. Available options: Single Stack or Dual Stack .
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address 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>Secondary IP</i>	<i>Select the IP address to open the secondary IP configuration panel for editing. This panel is available only when the stack type is set to Dual Stack.</i>
IP Address	The IP address assigned as the gateway address for the external traffic source.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i>). The default value is 000000000001.

Connectivity Settings	Description
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.

CoreSim configuration settings



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

The configuration settings are described in the topics listed below.

Topics:

Core settings	815
N6/SGi interface settings	816
AMF Ranges configuration settings	817
AMF node settings	819
AMF N2 interface settings	822
UPF Ranges configuration settings	823
UPF N3 interface settings	824
MME Ranges configuration settings	825
MME node settings	826
MME S1 interface settings	827
SGW Ranges configuration settings	828
SGW S1-u interface settings	829
SEG Ranges configuration settings	830
SEG interface settings	834

Core settings

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

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

Setting	Description
PLMN MCC	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	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.
Home Network Private Key	The Home Network Private key that is used for subscriber privacy.
Routing Indicators	<p><i>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.</i></p> <p><i>You can add as many Routing Indicators as necessary to support your test objectives.</i></p>
	Select the Add Routing Indicator button to add a Routing Indicator.
	Select the Delete button to remove the routing indicator.

N6/SGi interface settings

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

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

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

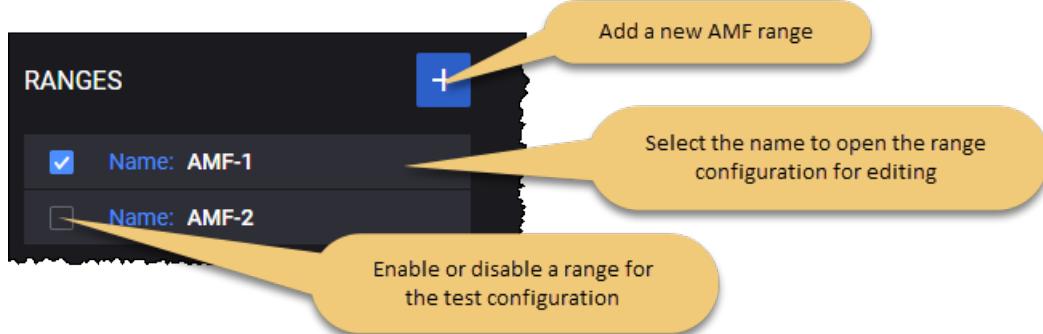
AMF Ranges configuration settings

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

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

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

For example ...



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

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

AMF range controls and settings

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

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

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

AMF node settings

Each AMF range includes a set of Node Settings.

Node Settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	<p>Multiple AMF instances may be deployed in the 5G network.</p> <p>Each AMF instance is uniquely identified by an <i>Instance ID</i>. You can accept the value provided by 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.
Relative Capacity	Set the relative capacity value.
Ciphering Algorithm	Allows to select the supported 5G ciphering algorithm: <ul style="list-style-type: none"> • NEA0 - Null ciphering algorithm • NEA1 - 128-bit SNOW 3G based algorithm • NEA2 - 128-bit AES based algorithm • NEA3 - 128-bit ZUC based algorithm
Integrity Algorithm	Allows to select the supported 5G integrity protection algorithm: <ul style="list-style-type: none"> • NIA0 - Null Integrity Protection algorithm • NIA1 - 128-bit SNOW 3G based algorithm • NIA2 - 128-bit AES based algorithm • NIA3 - 128-bit ZUC based algorithm
Request N2 SM Information	Enable this option to request N2 SM Information again instead of using the existing one.
Prefer AMF Change	Enable this option to change the AMF for an N2 handover even when the target RAN(T-RAN) is connected to the serving AMF.
<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>
Public Warning System	<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.

Public Warning System

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

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

AMF N2 interface settings

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

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

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

Connectivity Settings	Description
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>
VLAN ID	VLAN identifier.

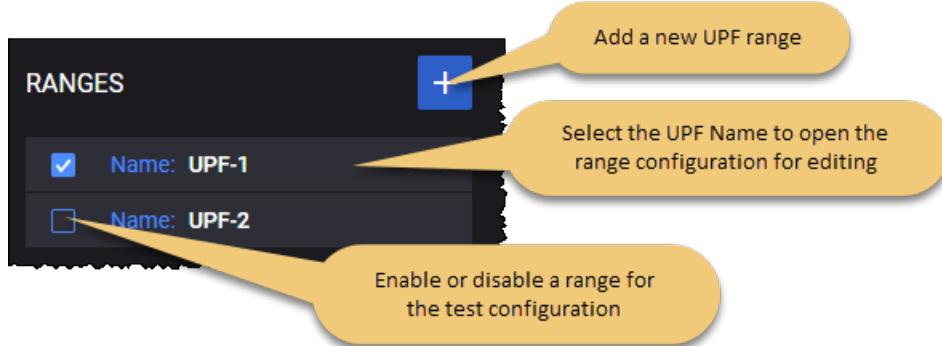
UPF Ranges configuration settings

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

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

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

For example ...



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

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

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

Setting	Description
<i>Range:</i>	
	Select the Delete Range button to delete this range from your test configuration.
Name	The name of the UPF range. You can accept the name provided by the 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 .

UPF N3 interface settings

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

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.

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

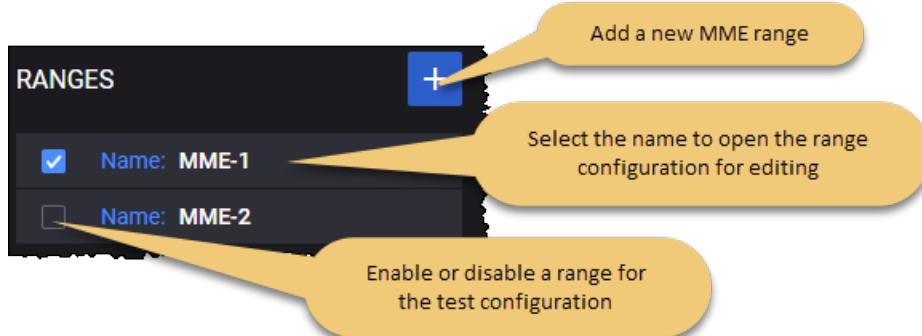
MME Ranges configuration settings

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

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

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

For example ...



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

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

MME range controls and settings

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

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

Setting	Description
Range:	

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

MME node settings

Each MME range includes a set of Node Settings.

Node Settings

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

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

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

MME S1 interface settings

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

S1 Interface Settings	Description
Local STCP Port	Set the local STCP port number.
<i>Connectivity Settings</i>	
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.

S1 Interface Settings	Description
MAC	Select the MAC address to open the MAC configuration panel for editing.
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<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.

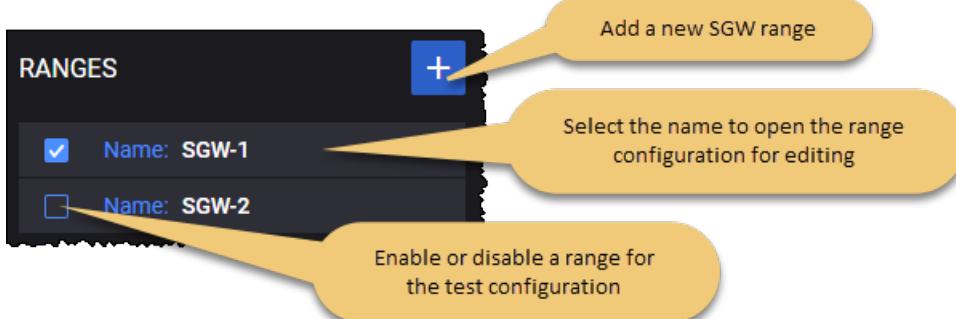
SGW Ranges configuration settings

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

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

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

For example ...



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

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

SGW range controls and settings

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

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

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

SGW S1-u interface settings

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

S1-u Interface Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.

S1-u Interface 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).
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.

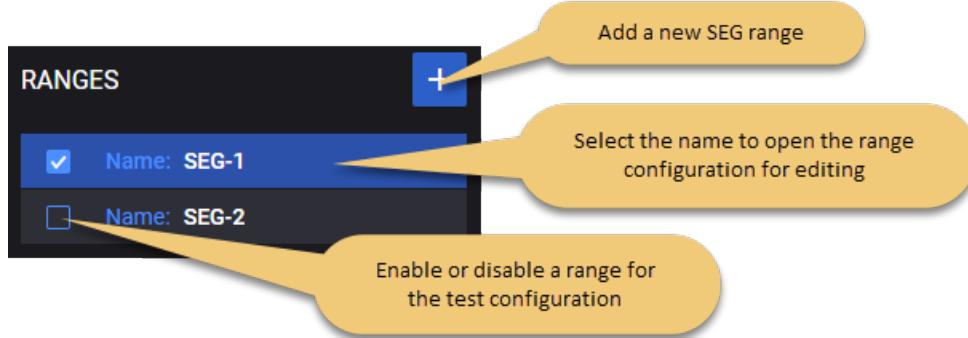
SEG Ranges configuration settings

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

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

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

For example ...



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

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

SEG range controls and settings

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

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

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

Setting	Description
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> minimum: 212992 maximum: 134217728 default: 2097152
<i>Interface Settings</i>	<i>These settings are described in SEG interface settings.</i>
<i>Remore Access IP Pool</i>	
Start IP	Set the start IP address.
IP Increment	Set the IP address increment value.
IPs count	Set the IP count value.
IP Prefix Length	Set the IP prefix length value.
<i>Local Protected Subnet</i>	<i>Selects which node(s) are protected by SEG: AMF and/or UPF . AMF and UPF could be protected by the same SEG when running with Linux stack.</i>
N2 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific AMF range from the list.
N3 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific UPF range from the list.
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to Certificates and cannot be changed.
CA Certificate	Select the CA certificate from the drop-down list.
Certificates and Private Keys (zip)	It allows you to upload an archive that contains the certificates and keys for the SEG range, using the Upload button. To remove the archive , select the Clear button. The .key and .crt files need to have the same name before extensions.
Use Same Certificates and Private Key For All Tunnels	By default, this option is disabled. Select the toggle button to enable it.
<i>IKE Phase 1</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: AES-128-GCM-16 . Available options: AES-128-CBC , AES-192-CBC , AES-256-CBC , AES-128-GCM-16 , AES-192-GCM-16 , AES-

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

Setting	Description
Type	Default value: ID_DER ASN1 DN . Available options: ID_IPV4_ADDR , ID_FQDN , ID_USER_FQDN , ID_IPV6_ADDR , ID_DER ASN1 DN , ID_KEY_ID .
Local Identification Value	Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: ID_FQDN , ID_KEY_ID or ID_RFC822_ADDR .
<i>Timers</i>	
Enable Rekey	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: 0 (disabled).
DDP Interval (s)	Set a value for this parameter. Default value: 0 (disabled).

SEG interface settings

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

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

SEG Interface Settings	Description
Increment	<i>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.</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.

CHAPTER 12

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	837
Passthrough test configuration notes	838

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

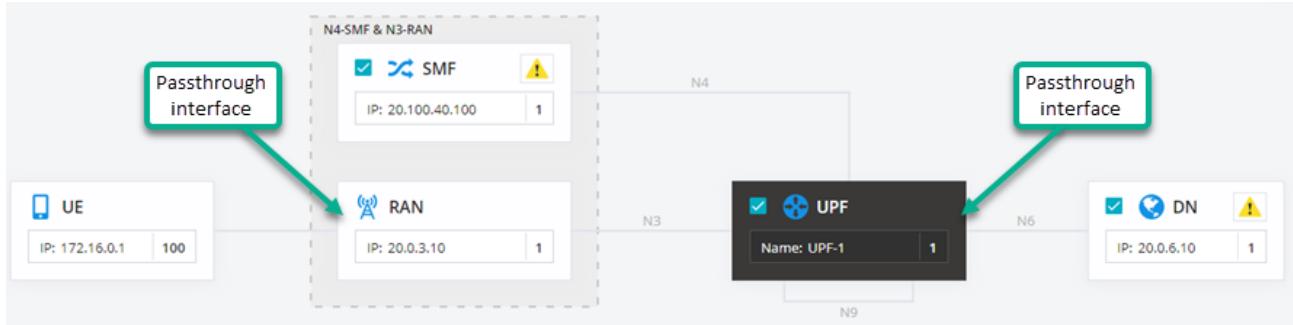
Both passthrough traffic and User Plane objectives traffic can work simultaneously. If you want only passthrough traffic, then there is no need to configure any traffic objectives.

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](#)
- [UE settings](#)
- [UPF settings](#)
- [N4-SMF & N3-RAN settings](#)
- [For more information](#)

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.
---	--

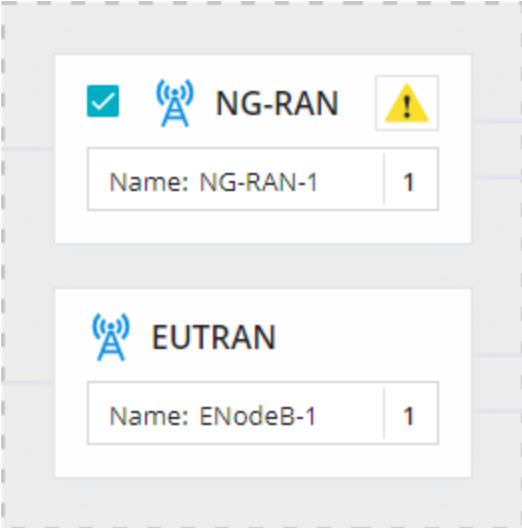
UPF settings

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](#)
- [UE Settings settings](#)
- [UPF N6 interface settings](#)

UPF Isolation:

- [Passthrough interface settings](#)
- [UE range settings](#)
- [UPF N6 interface settings](#)

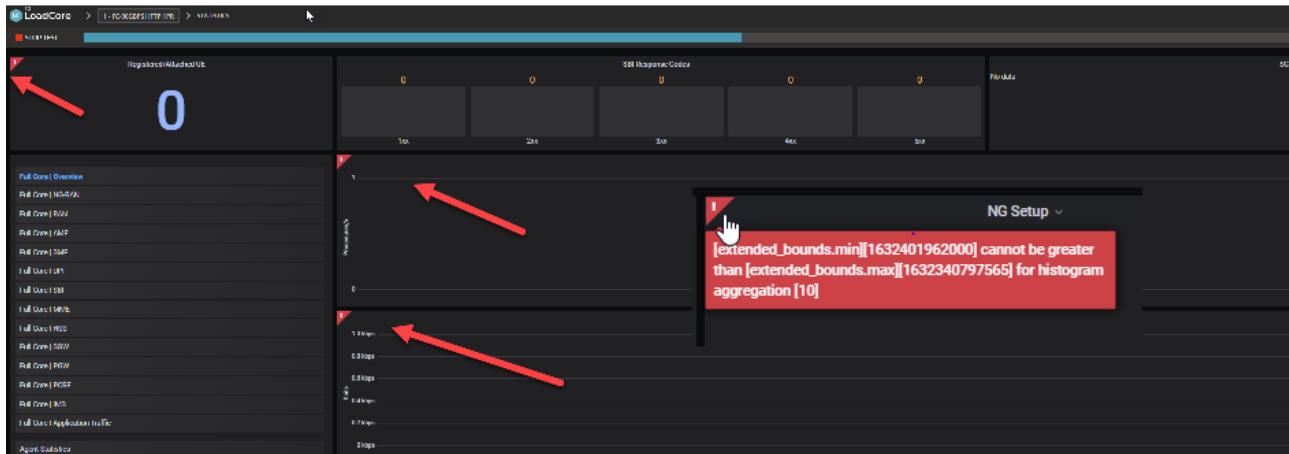
CHAPTER 13

Troubleshooting

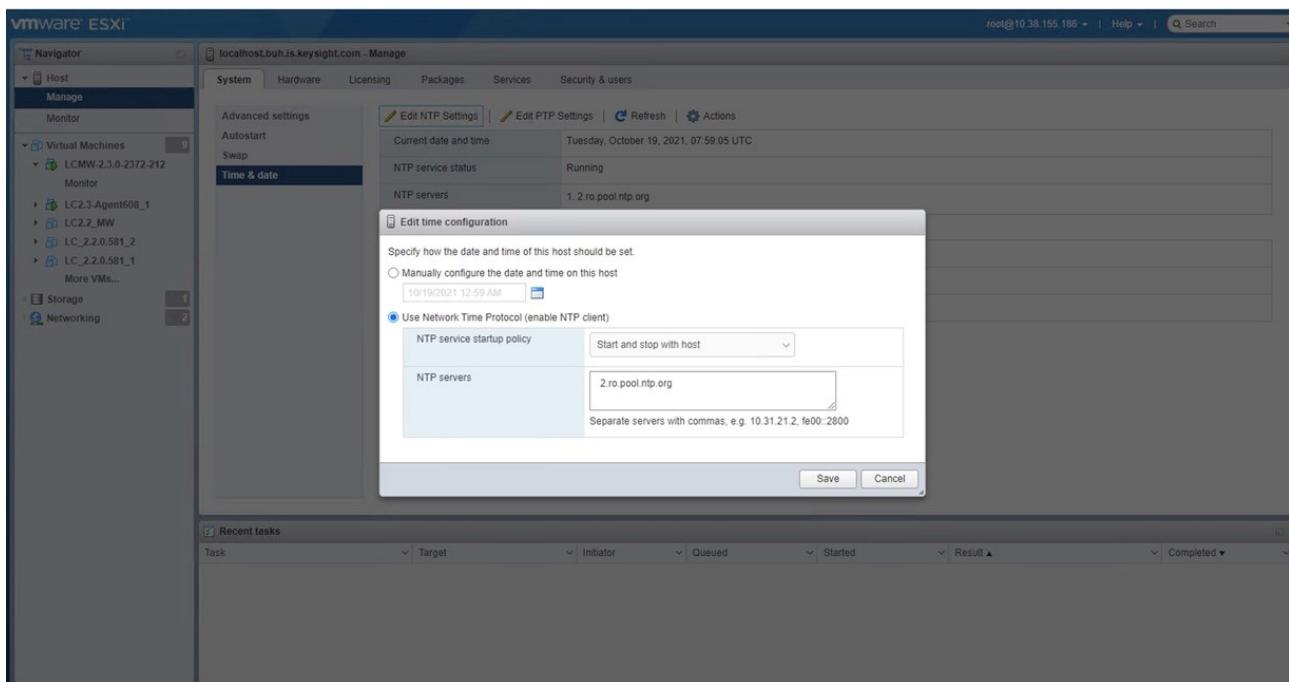
This section presents the most common errors or issues and their associated resolution (if available).

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
	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.
	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
YYLive		
Load Home Page	N/A	N/A
Select Category	Category	Provide the category.
Play Video	Video ID	Provide the Video ID.

The difference between Dynamic and Payload files

- If the chosen file is Payload (not Dynamic), the exact contents of the file can be seen on the wire.
- If the chosen file is Dynamic and the file does not contain Macros, then the behavior is the same as above.
- If the chosen file is Dynamic and the file contains Macros, then each Macro is evaluated during the test with the expected value that the Macro is meant to generate.

Artifacts

This section contains useful information and details on Playlist and Macro features.

Rules and Grammar for Playlists

Rules to support comma or double-quotes as a part of a playlist:

1. Each playlist item with comma or double-quote in the content **must** be enclosed within double-quotes.
2. Every double-quote used as a part of the content must be escaped with another double-quote.

Each record is located on a separate line, delimited by a line break (CRLF). For example: `record = value * (COMMA value)` :

Record	value 1	value 2
abcd	abcd	
abcd,wxyz	abcd	wxyz
"abcd,pqr","wxyz"	abcd,pqr	wxyz
"abcd,pq""r","wxyz"	abcd,pq"r	wxyz

For all applications that have a **Sign In** or **Sign Up** action, the following parameters offer the possibility of uploading a playlist file: Login Username, Login password or SignUp Username, SignUp password, SignUp confirm password. Select the **Playlist file** option and select the **Upload** option:

The screenshot shows the 'Traffic Profiles (1 application)' configuration screen. It includes three main sections: 'Applications' (listing 'eBanking Chrome to Apache 1' with a weight of 1), 'Actions' (listing 6 actions: Sign Up, Login, View Transactions, View Accounts, Get Contact Page, Logout), and 'Properties' (containing fields for 'Login username' (Playlist file, selected 'playlist (2).csv'), 'Login password' (User input, user1pass), and 'Upload' button).

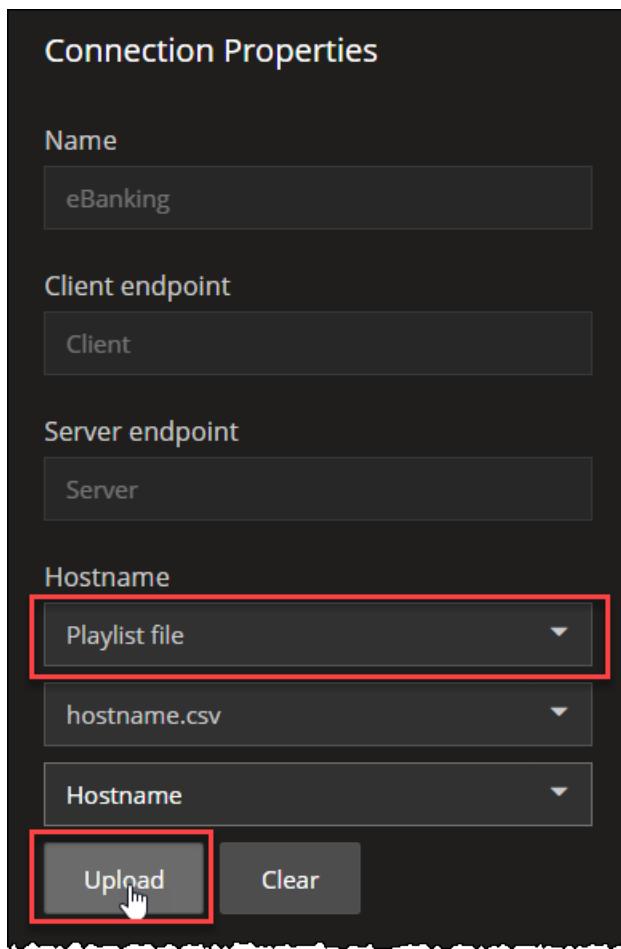
After the upload is performed, the reference column has corresponding csv column names, which can be chosen from the dropdown menu:

The screenshot shows the 'Actions' and 'Properties' tabs. In the 'Properties' tab, the 'Username' dropdown is highlighted with a red box, indicating it is the selected reference column for the 'Login username' field.

For some applications, the Hostname (under **ConnectionProperties**) offers the possibility of uploading a playlist file:

1. Select the **Playlist** file option .
2. Select **Upload**.

3. Choose the **Reference** column name from the drop-down.



Example of a Hostname playlist file:

NOTE As of now, we do not validate empty Hostname values, if they are fetched from a playlist file.

	A	B
1	Hostname	
2	server1.com	
3	server2.com	
4	server3.com	
5	server4.com	
6	server5.com	
7	server6.com	
8	server7.com	
9	server8.com	
10	server9.com	
11	server10.com	
12		
13		
14		
15		
16		
17		

About Playlists

For the **Sign In** action in eBanking, eShop, Social Network, Portal or the **Sign Up** action in eBanking applications, please use this [Sign In playlist](#) file:

	A	B	C	D	E	F	G	H	I
1	Username	Password							
2	admin	pgpassword							
3	michael	qwerty							
4	NULL	123456789							
5	john	12345							

For the **Sign In** action in Office 365 (Outlook, Excel, OneDrive) applications , please use this [Sign In Office 365 playlist](#) file:

	A	B	C	D	E	F	G	H
1	Username	Password	Email					
2	info	123456	info@example.com					
3	admin	pgpassword	admin@example.com					
4	michael	qwerty	michael@example.com					
5	NULL	12345zxs	NULL@example.com					
6	john	12345	john@example.com					
7	david	1234	david@example.com					
8	robert	111111	robert@example.com					
9	chris	1234567	chris@example.com					
10	mike	dragon	mike@example.com					

About Macros

A macro is a method or function which allows you to customize the payload text data with the following parameters. The `maxLength` limit is set to 1024:

Macros	Description
<code>\$(RandomIPAddress, 'IPv4')</code>	The RandomIPAddress macro randomly generates IPv4 address. IPv6 is not yet supported.
<code>\$(Rand, minValue, maxValue)</code>	The Rand macro generates one random number within the range [minValue, maxValue]. It takes one or two parameters. Range is 0 – N

	or N1 – N2.
<code>\$(RandomAscii, minLength, maxLength)</code>	The RandomAscii macro generates a sequence of random Ascii characters with values in the range: 0-127 minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomAlpha, minLength, maxLength)</code>	The RandomAlpha macro generates a sequence of random letters [A-Za-z]. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomNum, minLength, maxLength)</code>	The RandomNum macro generates a sequence of random digits minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomAlphaNum, minLength, maxLength)</code>	The RandomAlphaNum macro generates a sequence of random letters or digits [A-Za-z0-9]. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(RandomByte, minLength, maxLength)</code>	The RandomByte macro generates a sequence of random bytes. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
<code>\$(PatternRepeat, pattern, minLength, maxLength)</code>	The PatternRepeat macro generates a sequence of characters by repeating the <pattern> pattern. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length. If the chosen length is not an exact multiple of the length of <pattern>, the last repetition of <pattern> is truncated.

The following is the macro file structure, and please use this [macros](#) file for the correct file format:

```
dynamic_payload - Notepad
File Edit Format View Help
Random IPv4 $(RandomIPAddress, 'IPv4')
Random number between 200 and 400: $(Rand, 200, 400)
Random ascii $(RandomAscii, 10, 30)
Random alpha $(RandomAlpha, 5, 20)
RandomNum $(RandomNum, 10, 20)
Random Alpha Num $(RandomAlphaNum, 10)
Random Byte $(RandomByte, 2, 4)
Repeat pattern $(PatternRepeat, '!@#4QWEr', 5)
```

This feature is also available for the HTTP application, on both HTTP GET and HTTP POST actions, under the following parameters: Response body/Response body. Switch to the dynamic payload and upload the `dynamic_payload` file:

Assign the agents, enable capture and start the test. After the test is finished, download the captured information and you can see the payload, as set in the macro file:

No.	Time	Source	Destination	Protocol	Length	Info
16	0.099346	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 48737 → 88 [ACK] Seq=1 Win=2896 Len=0 TSval=764983045 TSecr=807789105
17	0.099359	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 37775 → 88 [ACK] Seq=1 Win=2896 Len=0 TSval=764983119 TSecr=807784865
18	0.099366	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 58394 → 88 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983026 TSecr=807847657
19	0.099374	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name=wall HTTP/1.1
20	0.099378	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name=wall HTTP/1.1
21	0.099378	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name=wall HTTP/1.1
22	0.099623	192.168.10.90	192.168.10.91	HTTP	590	HTTP/1.1 200 OK (text/plain)
23	0.099624	192.168.10.90	192.168.10.91	HTTP	682	HTTP/1.1 200 OK (text/plain)
24	0.099644	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 36116 → 88 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983171 TSecr=807846794
25	0.099651	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name=wall HTTP/1.1
26	0.099685	192.168.10.90	192.168.10.91	HTTP	582	HTTP/1.1 200 OK (text/plain)

```

> Frame 22: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)
> Ethernet II, Src: VMware_Aw6:29:b9 (00:0c:29:a6:29:b9), Dst: VMware_99:5a:02 (00:0c:29:99:5a:02)
> Internet Protocol Version 4, Src: 192.168.10.90, Dst: 192.168.10.91
> Transmission Control Protocol, Src Port: 80, Dst Port: 58394, Seq: 1, Ack: 306, Len: 524
> Hypertext Transfer Protocol
> Line-based text data: text/plain (12 lines)
Random IPv4 158.243.103.228\n\n
Random number between 208 and 400: 266\n\n
Random ascii: \016\035\035\023t\01..!\034+\031\030\026q\030\024<\r\n
Random alpha VEKZk\01..n
Random Num 227499253664034\r\n
Random Byte Y\01..n
Repeat pattern !@#4Q!Er!@#4Q!Er!@#4Q!Er!@#4Q!Er!\r\n
\r\n
\r\n
\r\n
\r\n

```

This page intentionally left blank.

Index

5

5G-EIR, configuration settings 389

A

Agent Assignment window 71

AMF, configuration settings 194

application traffic generator 155, 176, 179-180, 183, 246, 567, 589, 592-593, 631, 718, 740, 743-744, 747, 781

AUSF, configuration settings 210, 491

B

bidirectional UDP traffic flow 157, 569, 720

C

create/delete PDU session, secondary objective 151, 714

create/delete QoS Flows, secondary objective 149, 559, 712

customer assistance 3

D

discovery, NRF 393

DN, configuration settings 606

DNN settings

 Full Core tests 93, 663

 SBA tests 460

E

enter/exit idle, secondary objective 148, 558, 712

EPS fallback 308, 793

F

Full Core tests

 configuration settings 77

global settings 85, 658

network slicing 133, 700

objectives 137, 704

H

handover, secondary objective 556

I

IPFilterRule 541

M

middleware VM, upgrade 57

modify QoS Flows, secondary objective 559

N

Nnrf_NFDiscovery 393

NRF discovery 393

NRF, configuration settings 276, 500

O

objectives

 Full core tests 137, 704

 SBA tests 419

 UPF Isolation tests 551

P

packet filters

 for SDF 541

 packet filter list configuration 467

Paging, secondary objective 147, 557, 711

passthrough testing 836

PCF, configuration settings 290, 513

product support 3

Q

QoS flows, settings 100, 670

R

RAN, configuration settings 300, 634, 787

S

SBA tests

 configuration settings 396

 global settings 456

 network slicing 411

 objectives 419

SCP configuration settings 329, 519

SGW-U, configuration settings 381

SMF, configuration settings 346, 638

SMS, secondary objective 152

stateless UDP traffic generator 154, 227, 610, 717,
 763

T

TCP connection settings 457

technical support 3

traffic agents 71

traffic generators 153, 226, 564, 609, 715, 762

U

UDM, configuration settings 364, 523

UDP stateless, traffic generator 154, 227, 610, 717,
 763

UDR, configuration settings 377, 529

UE configuration settings

 Full Core tests 107, 677

 SBA tests 401

 UPF Isolation tests 543

UPF Isolation tests

 configuration settings 533

 global settings 536

objectives 551

UPF, configuration settings 381, 644

URRs 542



© Keysight Technologies, 2019–2023

This information is subject to change
without notice.

www.keysight.com