

# Keysight Open RAN Simulators, Cloud Edition 5.1

LoadCore

User Guide

# Notices

## Copyright Notice

© Keysight Technologies 2019–2025

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

## Warranty

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

## Technology Licenses

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

## U.S. Government Rights

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

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

## Contacting us

---

### Keysight headquarters

1400 Fountaingrove Parkway  
 Santa Rosa, CA 95403-1738  
 Email address: [support@keysight.com](mailto:support@keysight.com)  
 Website: <https://support.ixiacom.com/contact>

### Support

Location	Phone number	Local time
<i>Americas</i>		
US, Canada	1-888-829-5558	8h00 – 17h00
Brazil	0800-892-0522	8h00 – 17h00
Mexico	001-888-829-5558	8h00 – 17h00
Other	+1-719-273-6516	8h00 – 17h00
<i>EMEA</i>		
Belgium	0800-18686	8h30 – 17h30
Finland	0800-913-352	8h30 – 17h30
France	0800-917228	8h30 – 17h30
Germany	0800-0824099	8h30 – 17h30
India	1800-18-02552	8h30 – 17h30
Ireland	1800-949245	8h30 – 17h30
Israel	1-809-454975	8h30 – 17h30
Italy	0800-790571	8h30 – 17h30
Luxembourg	0800-25112	8h30 – 17h30
Netherlands	0800-022-9086	8h30 – 17h30

Romania	0213 015 699	8h30 – 17h30
Spain	800-654386	8h30 – 17h30
Sweden	0201-202266	8h30 – 17h30
United Kingdom	0800-0293882	8h30 – 17h30
<i>Asia and Australia</i>		
Australia	1-800-370-558	8h30 – 17h00
China Mainland	800-810-0005	8h30 – 17h30
	400-810-0005	8h30 – 17h30
Hong Kong	800-931-613	9h00 – 18h00
Japan	0120-421-621	9h00 – 17h30
Malaysia	1800-819 092	8h30 – 17h30
South Korea	080-770-0800	8h30 – 17h30
Singapore	800-101-3797	8h30 – 17h30
Taiwan	0800-699-880	9h00 – 18h00
Other	+65 6215 7600	8h30 – 17h30 (Singapore)

Last updated: 1 August 2024

# Table of Contents

---

<b>Contacting us .....</b>	<b>3</b>
<b>Chapter 1 Introduction .....</b>	<b>25</b>
<b>Chapter 2 Web Interface .....</b>	<b>26</b>
Access LoadCore Web UI .....	26
LoadCore Web UI .....	28
<b>Chapter 3 How Do I... .....</b>	<b>31</b>
Configure and run a test .....	32
Search Parameter .....	38
Manage and use test sessions .....	40
Save test sessions .....	41
Manage test sessions .....	41
Import and export sessions .....	44
Delete configs and sessions .....	45
Upgrade the MiddleWare VM .....	46
Configure Dashboard general settings .....	49
Work with Statistics .....	52
Debug .....	58
View Notifications and Test Events .....	58
Manage Test Results .....	60
Troubleshooting .....	61
<b>Chapter 4 Assign and manage agents .....</b>	<b>63</b>
About traffic agents .....	63
Assigning agents to nodes .....	63
Agent management .....	65
Network Management .....	68
Distribution Mode feature .....	69

<b>Chapter 5 Work with the Resource Library .....</b>	<b>73</b>
Import Captures .....	73
Create Custom Applications from Imported Captures .....	74
Edit Custom Applications .....	75
Export Custom Applications .....	76
Import Custom Applications .....	76
Procedures Resources (SIP/Media/Flow) .....	77
Procedures management .....	78
Procedures Library .....	79
Flow Editor .....	91
Debugging .....	96
UE Range Configuration .....	97
Dialog Handling .....	99
Non-blocking behavior .....	103
How to create and configure a procedure from scratch .....	105
Custom Fuzzing Scripts .....	108
Export Other Resources .....	108
Import Resources .....	108
<b>Chapter 6 Full Core tests: configuration settings .....</b>	<b>111</b>
Global Settings .....	120
Global Settings panel .....	122
Node Start/Stop Rates .....	122
DNS Settings .....	123
Advanced Settings .....	123
DNNs panel .....	127
DNN configuration settings .....	129
Session AMBR configuration settings .....	132
ePCO configuration settings .....	133
Traffic Control Settings configuration .....	134
3GPP RADIUS Server configuration .....	135
Impairment .....	136

QoS Flows panel .....	137
QoS Flow configuration settings .....	138
QoS Flow Packet Filter configuration settings .....	141
QoS Flow Max Packet Loss Rate settings .....	142
QoS Flow ARP configuration settings .....	142
QoS Flow MBR configuration settings .....	143
QoS Flow GBR configuration settings .....	143
CA Certificates .....	143
Milenage .....	144
Customer Parameters .....	145
External Stats Server .....	145
Global Playlists .....	152
UE configuration settings .....	153
UE Ranges panel .....	155
UE Range panel .....	156
Range Settings .....	158
UE Identification settings .....	159
UE Security settings .....	159
UE Settings settings .....	163
UE Shared Data IDs .....	171
UE Subscribed AMBR settings .....	171
Service Area Restriction settings .....	171
Forbidden Areas .....	173
DNNs Config .....	174
Notifications .....	177
SMS Configuration .....	177
Equipment Status .....	180
Converged Charging .....	180
Spending Limit Control .....	181
Internal Group IDs .....	184
Network Slicing settings .....	185

UE NSSAI settings .....	186
UDM Default NSSAI settings .....	187
UDM SNSSAI Mappings .....	187
UDR SNSSAI Settings .....	188
Objectives .....	189
Control Plane Objective .....	190
User Plane Objectives .....	206
3GPP RADIUS Server configuration settings .....	275
3GPP RADIUS Server Ranges panel .....	275
3GPP RADIUS Server Range settings .....	276
3GPP RADIUS Server Node settings .....	277
3GPP RADIUS Server N6 interface settings .....	277
AMF configuration settings .....	280
AMF Ranges panel .....	281
AMF Range settings .....	282
AMF Node settings .....	283
AMF Custom NF Services settings .....	286
AMF N2 interface settings .....	287
AMF Namf interface settings .....	290
AMF N26 Interface Settings .....	292
AMF Remote SBA nodes .....	293
AUSF configuration settings .....	301
AUSF Ranges panel .....	302
AUSF Range panel .....	302
AUSF Node settings .....	303
AUSF Nausf interface settings .....	304
AUSF Remote SBA Nodes .....	307
AUSF Custom NF Services settings .....	309
CHF configuration settings .....	310
CHF Ranges panel .....	310
CHF Range settings .....	311

CHF Node settings .....	312
CHF Nchf interface settings .....	313
CHF remote SBA nodes .....	315
DN configuration settings .....	317
DN Ranges panel .....	318
DN Range panel .....	318
DN N6 interface settings .....	319
DN routes settings .....	320
DN User Plane .....	321
DN Stateless UDP Traffic .....	322
DN Data Traffic .....	324
DN Voice Traffic .....	326
DN Video OTT Traffic .....	337
DN DNS Server Traffic .....	340
DN Predefined Applications Traffic .....	343
DN Capture Replay .....	343
DN Synthetic .....	345
DN UDG .....	347
DN Throttling settings .....	349
DNS Server configuration settings .....	350
DNS Server Ranges panel .....	350
DNS Server Range panel .....	350
DNS Server Ndnnserver interface settings .....	351
DNS Server Traffic Flow settings .....	352
EASDF configuration settings .....	355
EASDF Ranges panel .....	355
EASDF Range panel .....	356
EASDF Node settings .....	357
EASDF Neasdf interface settings .....	357
EASDF N6 interface settings .....	360
EASDF UE routes settings .....	360

EASDF DNS Server Settings .....	361
EASDF Custom NF Services settings .....	362
IMS configuration settings .....	364
CSCF Range panel .....	364
CSCF N6 interface settings .....	366
CSCF AF Interface settings .....	367
CSCF UE routes settings .....	370
Media Function Range panel .....	370
MME configuration settings .....	372
MME Ranges panel .....	373
MME Range panel .....	374
MME Node settings .....	375
MME S11 Interface Settings .....	377
MME N26 Interface Settings .....	378
MME S1 Interface Settings .....	380
MME S6a Interface Settings .....	381
MME Diameter settings .....	384
NEF configuration settings .....	386
NEF Ranges panel .....	386
NEF Range panel .....	387
NEF Node Settings .....	388
NEF Nnef interface settings .....	389
NEF Remote SBA Nodes .....	391
NEF Custom NF Services settings .....	393
NRF configuration settings .....	395
NRF Ranges panel .....	396
NRF Range panel .....	396
NRF Node settings .....	397
NRF Custom NF Services settings .....	398
NRF Nnrf interface settings .....	399
NRF Remote SBA Nodes .....	401

NSSF configuration settings .....	403
NSSF Ranges panel .....	404
NSSF Range panel .....	404
NSSF Node settings .....	405
Nnssf Interface Settings .....	406
Remote SBA nodes .....	409
NSSF Restricted NSSAIs .....	409
NSSF Network Slices .....	411
NSSF Configured NSSAI .....	412
PCF/PCRF configuration settings .....	413
PCF/PCRF Ranges panel .....	414
PCF Range panel .....	415
PCF Node settings .....	416
PCF Custom NF Services settings .....	418
PCRF Node settings .....	418
PCF service area restrictions .....	421
PCF Npcf interface settings .....	423
PCF remote SBA nodes .....	424
RAN configuration settings .....	426
gNodeB .....	427
gNodeB Ranges panel .....	428
gNodeB Range settings .....	433
gNodeB Node settings .....	434
gNodeB NSSAI settings .....	436
gNodeB N2 interface settings .....	437
gNodeB N3 interface settings .....	440
eNodeB .....	442
eNodeB Ranges panel .....	443
eNodeB Range Settings .....	447
eNodeB Node Settings .....	447
S1-U Interface Settings .....	449

S1-MME Interface Settings .....	450
Passthrough interface settings .....	453
SBI Fuzzer configuration settings .....	455
SBI Fuzzer Ranges panel .....	455
SBI Fuzzer Range panel .....	456
SBI Node Settings .....	457
SBI Fuzzer interface settings .....	459
SBI Fuzzer Target Node .....	461
SCP configuration settings .....	463
SCP Ranges panel .....	463
SCP Range panel .....	464
SCP Node Settings .....	465
SCP Nscp interface settings .....	465
SCP Remote SBA Nodes .....	468
SEPP configuration settings .....	470
SEPP Ranges panel .....	470
SEPP Range panel .....	471
SEPP Node Settings .....	472
SEPP Custom NF Services settings .....	473
SEPP Nsepp interface settings .....	473
SEPP Remote SBA Nodes .....	476
SGW configuration settings .....	478
SGW Ranges panel .....	479
SGW Range panel .....	480
SGW S1-U Interface Settings .....	481
SGW S5-C Interface Settings .....	482
SGW S5-U Interface Settings .....	483
SGW S11 Interface Settings .....	484
SGW DUT S11 Interface Settings .....	485
SMF/PGW-C configuration settings .....	486
SMF/PGW-C Ranges panel .....	487

SMF/PGW-C Range settings .....	488
SMF Node settings .....	489
SMF Custom NF Services settings .....	491
SMF N4/Sx interface settings .....	491
SMF Nsmf interface settings .....	493
SMF Gx Interface settings .....	496
SMF S5-c interface settings .....	499
SMF remote SBA nodes .....	500
SMF Uplink Paths settings .....	505
SMF Slice and UPF Mapping settings .....	506
SMF EAS Deploy Subscription settings .....	506
SMF EAS Procedures Settings .....	507
SMSF configuration settings .....	509
SMSF Ranges panel .....	509
SMSF Range panel .....	510
SMSF Node settings .....	511
SMSF Nsmsf interface settings .....	511
SMSF Remote SBA Nodes .....	514
UDM/HSS configuration settings .....	518
UDM/HSS Ranges panel .....	519
UDM/HSS Range panel .....	520
UDM Range Settings .....	521
UDM Settings .....	521
UDM Node Settings .....	522
UDM/HSS Custom NF Services settings .....	525
UDM Nudm Interface Settings .....	526
UDM Remote SBA Nodes .....	528
HSS Range Settings .....	530
HSS Settings .....	530
HSS Node Settings .....	531
HSS S6a Interface Settings .....	532

UDM and HSS Range Settings .....	534
UDM/HSS Custom NF Services settings .....	535
UDR configuration settings .....	537
UDR Ranges panel .....	537
UDR Range panel .....	538
UDR Node Settings .....	539
UDR Nudr interface settings .....	539
UDR Remote SBA Nodes .....	542
UDR Custom NF Services settings .....	542
UPF/PGW-U configuration settings .....	544
UPF/PGW-U Ranges panel .....	545
UPF/PGW-U Range panel .....	546
UPF Node settings .....	547
UPF N3 interface settings .....	547
UPF N4 interface settings .....	549
UPF N6 interface settings .....	550
UPF N9 interface settings .....	551
UPF Nupf Interface Settings .....	553
UPF N4u interface settings .....	554
UPF Remote SBA Nodes .....	556
UPF Slice Mapping settings .....	556
5G-EIR configuration settings .....	558
5G-EIR Ranges panel .....	558
5G-EIR Range panel .....	559
5G-EIR Node settings .....	559
5G-EIR N5g-eir interface settings .....	560
5G-EIR Remote SBA Nodes .....	562
NF Discovery service .....	563
<b>Chapter 7 NG-RAN Simulation tests .....</b>	<b>565</b>
<b>Chapter 8 SBA tests: configuration settings .....</b>	<b>566</b>
SBA Tester overview .....	570

UE configuration settings .....	571
UE Ranges panel .....	572
UE Range panel .....	572
Range Settings .....	573
UE Identification .....	574
UE Security .....	575
UE Settings .....	577
UE SDF settings .....	578
Shared Data IDs .....	579
UE Subscribed AMBR settings .....	579
Service Area Restrictions .....	580
Forbidden Areas .....	581
Notifications .....	581
SMS Configuration .....	582
Network Slicing .....	584
UDM Default NSSAI settings .....	585
UDM SNSSAI Mappings .....	585
UDR SNSSAI Settings .....	586
Charging Function .....	587
Converged Charging .....	587
Spending Limit Control .....	588
Objectives .....	591
Primary Objective .....	592
Secondary Objectives .....	631
SBA Tester Global Settings panel .....	658
Connection Settings .....	660
Advanced Settings .....	660
Impairment .....	662
DNNs panel .....	663
DNN configuration settings .....	664
DNN GBR configuration settings .....	665

Session AMBR configuration settings .....	666
QoS Flows panel .....	667
QoS Flow configuration settings .....	668
QoS Flow Packet Filter configuration settings .....	670
QoS Flow Maximum Packet Loss configuration settings .....	671
QoS Flow ARP configuration settings .....	671
QoS Flow MBR configuration settings .....	672
QoS Flow GBR configuration settings .....	672
External Stats Server .....	672
SBA Tester Simulated Nodes panel .....	680
AMF configuration settings .....	680
SMF configuration settings .....	686
PCF configuration settings .....	691
AF configuration settings .....	696
SBA Tester Remote SBA Nodes .....	702
SBA Tester Remote Nodes .....	704
AUSF configuration settings .....	706
AUSF Ranges panel .....	707
AUSF Range panel .....	707
AUSF node settings .....	708
AUSF Nausf interface settings .....	709
AUSF remote SBA nodes .....	710
CHF configuration settings .....	712
CHF Ranges panel .....	712
CHF Range panel .....	713
CHF node settings .....	713
CHF Nchf interface settings .....	714
CHF remote SBA nodes .....	715
NRF configuration settings .....	716
NRF Ranges panel .....	716
NRF Range panel .....	716

NRF node settings .....	717
NRF Nnrf interface settings .....	718
NSSF configuration settings .....	720
NSSF Ranges panel .....	721
NSSF Range panel .....	721
NSSF node settings .....	722
Nnssf Interface Settings .....	723
Remote SBA nodes .....	724
NSSF Restricted NSSAIs .....	725
NSSF Network Slices .....	726
NSSF Configured NSSAI .....	727
PCF configuration settings .....	728
PCF Ranges panel .....	728
PCF Range panel .....	728
PCF node settings .....	729
PCF service area restrictions .....	731
PCF Npcf interface settings .....	732
PCF remote SBA nodes .....	733
SCP configuration settings .....	734
SCP Ranges panel .....	734
SCP Range panel .....	735
SCP Nscp interface settings .....	736
SCP Remote SBA Nodes .....	737
SMSF configuration settings .....	738
SMSF Ranges panel .....	738
SMSF Range panel .....	739
SMSF node settings .....	740
SMSF Nsmsf interface settings .....	740
SMSF Remote SBA Nodes .....	741
UDM configuration settings .....	744
UDM Ranges panel .....	744

UDM Range panel .....	745
UDM node settings .....	746
UDM Nudm interface settings .....	749
UDM remote SBA nodes .....	750
UDR configuration settings .....	751
UDR Ranges panel .....	751
UDR Range panel .....	752
UDR Nudr interface settings .....	754
UDR remote SBA nodes .....	755
<b>Chapter 9 UPF Isolation tests: configuration settings .....</b>	<b>756</b>
Global Settings panel .....	758
DNS Settings .....	759
Advanced Settings .....	759
Impairment .....	762
QoS Flows panel .....	763
QoS Flow configuration settings .....	763
Reporting Settings .....	765
External Stats Server .....	765
Global Playlists .....	772
UE configuration settings .....	774
UE Ranges panel .....	775
UE Range panel .....	776
UE range settings .....	777
Objectives .....	783
Control Plane Objective .....	783
User Plane Objectives .....	796
RAN configuration settings .....	851
RAN Ranges panel .....	852
RAN Range settings .....	852
RAN N3 interface settings .....	853
Passthrough interface settings .....	854

SMF configuration settings .....	855
SMF Ranges panel .....	856
SMF Range settings .....	856
SMF N4 interface settings .....	857
SMF Uplink Paths .....	859
UPF configuration settings .....	861
UPF Ranges panel .....	862
UPF Range panel .....	862
UPF N3 interface settings .....	863
UPF N4 interface settings .....	865
UPF N6 interface settings .....	866
UPF N9 interface settings .....	867
UPF N4u interface settings .....	869
DN configuration settings .....	872
DN Ranges panel .....	872
DN Range panel .....	873
DN N6 Interface settings .....	874
DN routes settings .....	875
DN User Plane .....	876
DN Stateless UDP Traffic .....	877
DN Data Traffic .....	878
DN Voice Traffic .....	881
DN Video OTT Traffic .....	894
DN DNS Server Traffic .....	897
DN Predefined Applications Traffic .....	899
DN Capture Replay .....	899
DN Synthetic .....	901
DN UDG .....	903
DN Throttling settings .....	905
<b>Chapter 10 IP Endpoints tests: configuration settings .....</b>	<b>907</b>
Global Settings .....	909

DNS Settings .....	909
Advanced Settings .....	910
UDP Buffer Settings .....	912
Impairment .....	912
Milenage .....	912
External Stats Server .....	913
Global Playlists .....	920
IP Client configuration settings .....	922
IP Client Ranges panel .....	922
IP Client Range panel .....	923
IP Client interface settings .....	924
IP Client Timeline .....	925
IP Client User Plane .....	925
Stateless UDP Traffic .....	926
Data Traffic .....	927
Voice Traffic .....	931
Video OTT Traffic .....	946
DNS Client Traffic .....	950
ICMP Client .....	953
Capture Replay .....	954
Synthetic .....	955
UDG .....	957
REST API Client .....	961
Triple Play Server configuration settings .....	966
CSCF Range panel .....	966
Media Function Range panel .....	967
Data/Video configuration settings .....	968
Data/Video Ranges panel .....	969
Data/Video Range panel .....	969
Data/Video interface settings .....	970
Data/Video User Plane .....	971

Data/Video Throttling settings .....	998
<b>Chapter 11 IPsec NG-RAN tests: configuration settings .....</b>	<b>999</b>
Global Settings .....	1002
Global Settings panel .....	1003
Node Start/Stop Rates .....	1004
DNS Settings .....	1004
Advanced Settings .....	1005
DNNs panel .....	1008
DNN configuration settings .....	1008
Session AMBR configuration settings .....	1012
ePCO configuration settings .....	1012
Traffic Control Settings configuration .....	1014
Impairment .....	1015
QoS Flows panel .....	1016
QoS Flow configuration settings .....	1016
QoS Flow Packet Filter configuration settings .....	1020
QoS Flow Max Packet Loss Rate settings .....	1021
QoS Flow ARP configuration settings .....	1021
QoS Flow MBR configuration settings .....	1022
QoS Flow GBR configuration settings .....	1022
Milenage .....	1022
Customer Parameters .....	1023
CA Certificates .....	1023
External Stats Server .....	1024
Global Playlists .....	1031
UE configuration settings .....	1031
UE Ranges panel .....	1032
UE Range panel .....	1033
Range Settings .....	1034
UE Identification settings .....	1034
UE Settings settings .....	1035

UE Security settings .....	1057
UE Subscribed AMBR settings .....	1061
DNNs Config .....	1062
SMS Configuration .....	1064
Untrusted WiFi Settings .....	1065
Network Slicing settings .....	1067
UE NSSAI settings .....	1068
UDM SNSSAI Mappings .....	1069
Objectives .....	1069
Control Plane Objective .....	1069
User Plane Objectives .....	1082
DN configuration settings .....	1130
DN Ranges panel .....	1131
DN Range panel .....	1131
DN N6 interface settings .....	1132
DN routes settings .....	1133
DN User Plane .....	1134
DN Stateless UDP Traffic .....	1135
DN Data Traffic .....	1137
DN Voice Traffic .....	1139
DN Video OTT Traffic .....	1150
DN DNS Server Traffic .....	1153
DN Predefined Applications Traffic .....	1156
DN Capture Replay .....	1156
DN Synthetic .....	1158
DN Throttling settings .....	1160
IMS configuration settings .....	1160
CSCF Range panel .....	1161
Media Function Range panel .....	1162
RAN/Untrusted AP configuration settings .....	1162
gNodeB .....	1163

gNodeB Ranges panel .....	1163
gNodeB Range settings .....	1167
gNodeB node settings .....	1168
gNodeB NSSAI settings .....	1170
gNodeB N2 interface settings .....	1172
gNodeB N3 interface settings .....	1176
 eNodeB .....	1180
eNodeB Ranges panel .....	1180
eNodeB Range Settings .....	1184
eNodeB Node Settings .....	1185
S1-U Interface Settings .....	1186
S1-MME Interface Settings .....	1187
UNAP .....	1190
UNAP Ranges panel .....	1190
UNAP Range Settings .....	1191
Passthrough interface settings .....	1193
SEG/N3IWF & Core configuration settings .....	1195
Core settings .....	1195
N6/SGi interface settings .....	1197
Core Ranges settings .....	1198
AMF Ranges configuration settings .....	1198
UPF Ranges configuration settings .....	1208
MME Ranges configuration settings .....	1210
SGW Ranges configuration settings .....	1219
SEG Ranges configuration settings .....	1222
SEG interface settings .....	1226
N3IWF Ranges configuration settings .....	1226
N3IWF interface settings .....	1233
 <b>Chapter 12 Manage LoadCore licenses .....</b>	<b>1239</b>
Licensing Requirements .....	1239
License Manager .....	1239

License Server .....	1241
Licensed Test Configs .....	1242
<b>Chapter 13 Manage LoadCore users .....</b>	<b>1261</b>
Reset Password for Regular Users .....	1263
Configure LoadCore with LDAP/AD .....	1265
<b>Chapter 14 Passthrough testing .....</b>	<b>1271</b>
Overview of passthrough testing .....	1272
Passthrough test configuration notes .....	1273
<b>Appendix A 5G abbreviations .....</b>	<b>1275</b>
<b>Appendix B Predefined Applications .....</b>	<b>1281</b>
<b>Appendix C Application Actions .....</b>	<b>1295</b>
<b>Index .....</b>	<b>1351</b>

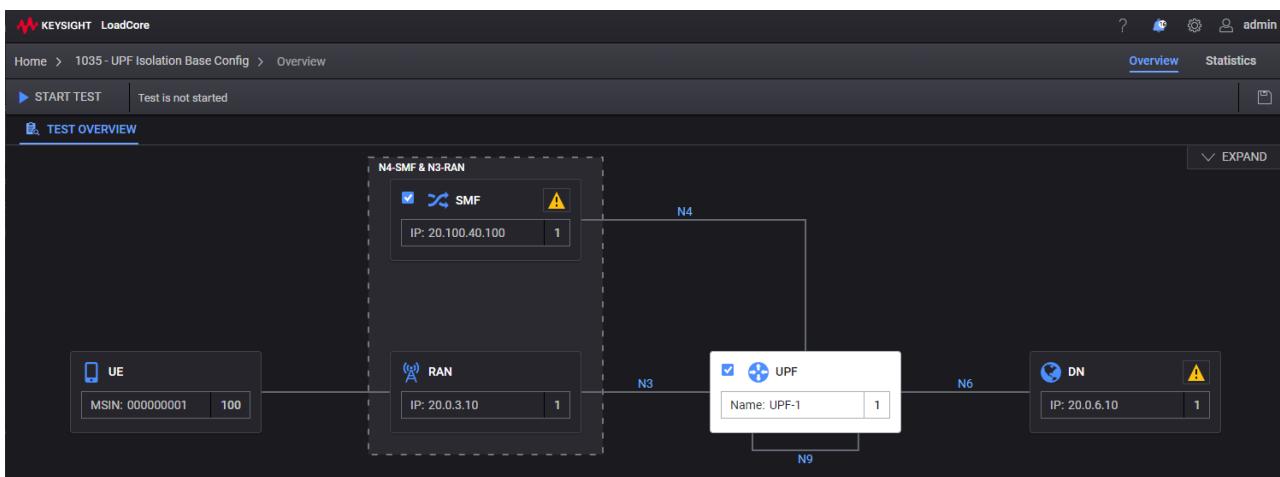
## CHAPTER 1

# 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*

## 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:

<b>Access LoadCore Web UI .....</b>	<b>26</b>
<b>LoadCore Web UI .....</b>	<b>28</b>

### Access LoadCore Web UI

This chapter describes the actions that are required the first time you log in to LoadCore as the application administrator, following deployment.

- [Required information below](#)
- [Initial login and password change below](#)
- [Activate licenses using License Manager on the next page](#)
- [Configure the License Server on page 28](#)
- [Create regular user accounts on page 28](#)

#### Required information

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

#### Initial login and password change

LoadCore provides a default administrator account, and you will use that account on your initial login and for subsequent administrative tasks.

To log in as the administrator:

1. Enter the IP address of your deployed LoadCore instance in your browser's address field.  
LoadCore opens the Keysight login page.
2. Enter the default administrator login credentials:
  - user ID: **admin**
  - password: **admin**

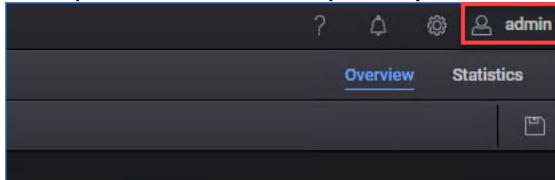
3. Click **Login**.

Because this is the initial login, LoadCore requires that you change the password for the admin account.

4. Review and accept the Keysight Software End User License Agreement.

5. Change the default **admin** user password:

- Click your account name (*admin*) in the LoadCore title bar.



LoadCore opens the **Edit Account** page in a new browser tab.

- Click **Password** in the navigation pane.
- Enter the current password and your new password.
- Click **Save**.

Next steps:

- Activate licenses
- Configure your license server
- Create user accounts

## Activate licenses using License Manager

Once you have completed the initial admin login, you need to activate the licenses for this LoadCore deployment.

To activate your licenses:

- Select **Administration** from the setup menu (⚙).
  - Select **License Manager** from the **Administration** menu. LoadCore opens the **License Manager** page.
  - To activate your licenses:
    - Select **Activate licenses**.  
LoadCore opens the **Activate Licenses** dialog.
    - Enter your license data in the dialog box.  
You can use either activation codes or entitlement codes (one or more ).
    - Select **Load Data**, indicate the number of licenses you want to activate, then click **Activate**.
- Your new licenses—which should now be listed in the **License Manager** page—are now available for running tests.

## Configure the License Server

If you are using an external License server, then you need to select and configure your license provider:

1. Select **Applications Settings** from the setup menu (⚙).  
LoadCore opens the **Application Settings** dialog.
2. Select your **License Provider** from the drop-down list:
  - **Legacy License Server** - this option is set by default on LoadCore (using the old LicenseManager).
  - **External License Server** - select this option to set an external license server (using the new LicenseManager 1.7).
  - **Embedded License Server** - the license server that is included in the middleware.
3. Enter the **License Server IP** address (see [Required information on page 26](#), above).
4. Click **Update**.

## Create regular user accounts

Before you and other members of your organization start building and running tests, it is recommended that you—logged in as the administrator—create a *regular user account* for each individual (including yourself). Further, it is recommended that you use the admin account only for administrative activities.

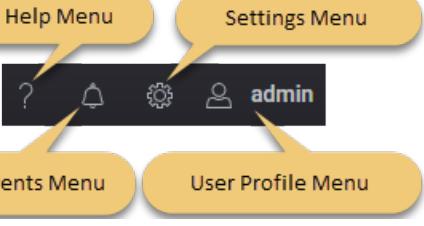
Refer to [Manage CoreSIM users](#) for detailed information about user account management.

## 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 <b>Help Menu</b> 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>

Section	Description
	<ul style="list-style-type: none"> <li>Access <b>LoadCoreHelp</b> where you can find info about the official LoadCore documentation and access the Rest API Browser.</li> <li>Access <b>Technical Support</b> section, where you can do the following: <ul style="list-style-type: none"> <li><b>Contact Keysight</b></li> <li><b>Collect diagnostics</b> - for more details refer to <a href="#">Collect Diagnostics</a>.</li> <li><b>EULA</b> - select this option to revisit and accept Keysight Software End User License agreement.</li> <li>Access <b>My software support...</b></li> <li><b>About LoadCore...</b> - this option displays details regarding the LoadCore software version.</li> </ul> </li> </ul> <p>The <b>Events Menu</b> can be accessed by selecting the bell icon on the top right corner of the Dashboard page. Here you can <a href="#">view notifications and test events</a>.</p> <p>The <b>Settings Menu</b> 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"> <li><b>License Manager</b> - select this option to open the <a href="#">License Manager</a> section.</li> <li><b>Agent Management</b> - select this option to open the <a href="#">Traffic agents management</a> section.</li> <li><b>Software Updates</b> - select this option to open the <a href="#">Software Updates</a> section.</li> <li><b>Application settings</b> - select this option set or update the license server IP. For more details, refer to <a href="#">Dashboard General Settings</a>.</li> <li><b>Logs Level</b> - select this option to collect logs info. For more details, refer to <a href="#">Dashboard General Settings</a>.</li> <li><b>Data migration</b> - select this option to open the data migration tool. For more details, refer to <a href="#">Dashboard General Settings</a>.</li> <li><b>System Monitor</b> - select this option to open the system monitor tool. For more details, refer to <a href="#">Dashboard General Settings</a>.</li> <li><b>User Management</b> - select this option to open the <a href="#">Access Control</a> section. This section handles server administration security configuration and also all the users settings. For more information on the Access Control options and configuration, refer to the official <a href="#">Keycloak documentation</a>.</li> </ul> <p>The <b>User Profile Menu</b> 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"> <li>Access and review your user profile.</li> <li>Change LoadCore Dashboard theme. For more details, refer to <a href="#">Dashboard General Settings</a>.</li> <li><b>Log Out</b> - select this option to log out of LoadCore. For more details, refer to <a href="#">Dashboard General Settings</a>.</li> </ul>
Test sessions	This section displays your current test sessions. Each test session can be accessed by selecting it.

<b>Section</b>	<b>Description</b>
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"> <li>• Core topology: <ul style="list-style-type: none"> <li>▪ Wireless Full Core</li> <li>▪ Wireless IP Endpoints</li> <li>▪ Wireless IPsec NG-RAN</li> <li>▪ Wireless UPF Isolation</li> <li>▪ Wireless SBA</li> <li>▪ Wireless NG-RAN Simulation</li> </ul> </li> </ul> <p>Selecting one of the options above will create a new session with that type of topology loaded. The steps required for configuration are described in the <a href="#">Configure and run a test</a> section.</p>
Browse Configs	<p>This section allows you to manage previously configured test sessions. By selecting the <b>Browse Configs</b> button, you can perform additional test related actions:</p> <ul style="list-style-type: none"> <li>• open a new base configuration test</li> <li>• delete test configurations</li> <li>• save test configurations</li> <li>• import and export test configurations</li> </ul> <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 3***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:

<b>Configure and run a test</b>	<b>32</b>
Search Parameter	38
<b>Manage and use test sessions</b>	<b>40</b>
Save test sessions	41
Manage test sessions	41
Import and export sessions	44
Delete configs and sessions	45
<b>Upgrade the MiddleWare VM</b>	<b>46</b>
<b>Configure Dashboard general settings</b>	<b>49</b>
<b>Work with Statistics</b>	<b>52</b>
<b>Debug</b>	<b>58</b>
View Notifications and Test Events	58
Manage Test Results	60
Troubleshooting	61

## 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 IP Endpoints test](#)
- [Configure a Wireless UPF Isolation test](#)
- [Configure a Wireless SBA test](#)
- [Configure Wireless NG-RAN Simulation test](#)
- [Configure Wireless IPsec NG-RAN 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 enabling the **Device Under Test** option, 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 \(UPF/PGW-U\)](#)

To locate specific parameters within the test session, use the [Search](#) functionality.

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 Wireless IP Endpoints test

To configure this test, do the following:

1. On the LoadCore Dashboard page, under the Create New Test section, select **Wireless IP Endpoints**.  
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 enabling the **Device Under Test** option, 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:

- [Triple Play Server](#)

To locate specific parameters within the test session, use the [Search](#) functionality.

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 IP clients. While there are a large number of IP clients configuration settings, you can often use the default values with little or no modification.  
For IP clients configuration, refer to [IP Clients](#).
7. On the [IP Clients](#), configure the test objectives.  
The User Plane Objectives determine the behavior of the simulated IP clients.
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 enabling the **Device Under Test** option, 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 \(UPF\)](#)

To locate specific parameters within the test session, use the [Search](#) functionality.

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 enabling the **Device Under Test** option, 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 \(SCP\)](#)
- [Short Message Service Function \(SMSF\)](#)
- [Unified Data Management \(UDM\)](#)
- [Unified Data Repository \(UDR\)](#)

To locate specific parameters within the test session, use the [Search](#) functionality.

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 IPsec NG-RAN test

To configure this test, do the following:

1. On the LoadCore Dashboard page, under the Create New Test section, select **Wireless IPsec NG-RAN**.  
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 enabling the **Device Under Test** option, 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:

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

To locate specific parameters within the test session, use the [Search](#) functionality.

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.

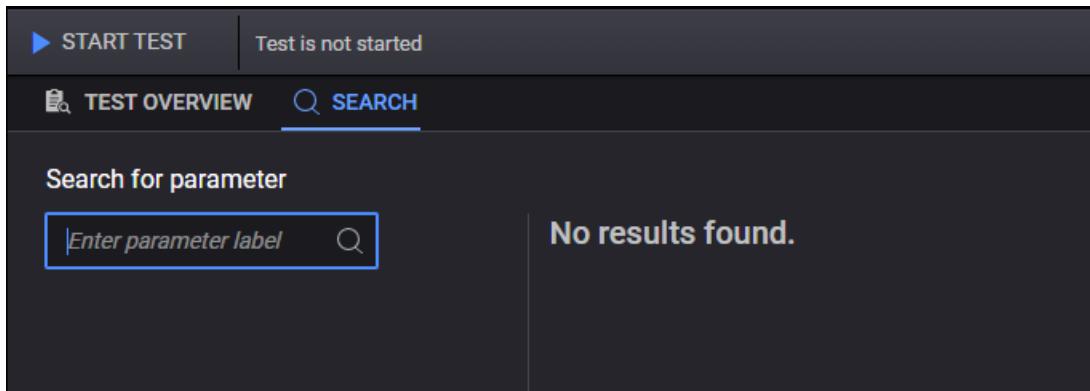
Once the test is running, you can click or tap **Statistics** to start monitoring the progress of the test.

**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.

## Search Parameter

The Search option is situated adjacent to the Test Overview tab within the application's user interface.



The parameter Search functionality enables users to locate specific parameters within a test session. This feature assists in identifying paths where a parameter is configured, aiding navigation and configuration processes.

**IMPORTANT**

This functionality is exclusive to the test session level and does not extend its search functionality to other sessions or topologies open in the application.

To use the Search functionality, select the **Search** tab and specify the name of the parameter into the **Search for parameter** field.

Upon entering the parameter name (for example, *plmn*), the search generates a list of paths where the parameter is configured within the topology.

The screenshot shows a search interface with a search bar containing 'plmn'. Below the search bar, it says '(37 results)'. To the right, there is a list of 5 search results, each with a small icon and a path description:

- RAN → gNodeB → ranges → [1] → Node Settings → PLMN MCC
- RAN → eNodeB → ranges4G → [100000] → Node Settings → PLMN MCC
- AMF → ranges → [1] → Node Settings → PLMN MCC
- AMF → ranges → [1] → Remote SBA Nodes → PLMN MCC
- SMF/PGW-C → ranges → [1] → Node Settings → PLMN MCC

Each result displays the path(s) within the topology where the parameter can be configured.

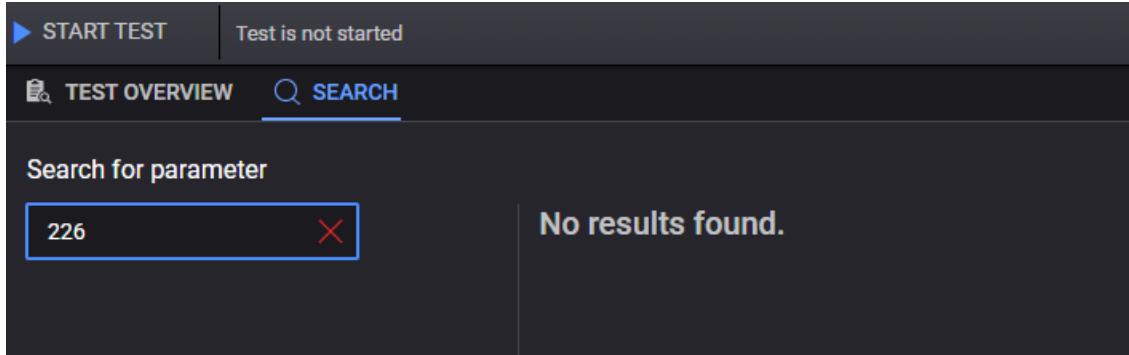
Clicking on any of the displayed paths enables users to navigate directly to that specific path within the topology.

The screenshot shows the RAN configuration interface for a gNodeB. On the left, a sidebar lists 'gNodeB' (selected), 'eNodeB', and 'Passthrough Interface Settings'. The main area is titled 'Ranges Connectivity' and contains a 'RANGES' section with a 'Name: gNodeB-1' entry. To the right, there are several configuration tabs and input fields:

- RANGE** tab: Device Under Test (switch off), Range Count (1).
- Node Settings** tab (selected):
  - Name: gNodeB-1
  - PLMN MCC: 226
  - PLMN MNC: 04
  - Tracking Area Code: 1011
  - gNodeB ID: 78
  - gNodeB ID Length: 22
  - Cell ID: 1
  - Connection Timeout (ms): 1000
  - Perform Load Balancing (switch off)
- EPS Fallback Settings** tab:
  - Enable EPS Fallback (checkbox off)
  - User Plane Security (checkbox off)
  - Public Warning System (checkbox off)

## Limitations

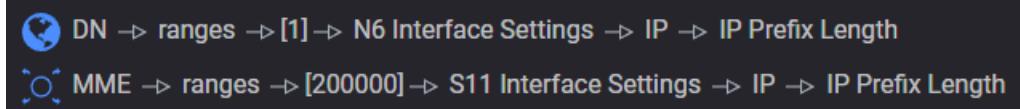
- **Search Functionality:** Supports searching for parameters to be configured but not for the values of those parameters. For example, searching for the value 226 will not return any results.



- **Highlighting:** The searched parameter within the search results or selected path is not highlighted.

## Additional Information

- **Matched Results Display:** The number of matched results is exhibited below in the search field.
- **Lists and Indices:** In cases of lists, the index displayed in the result path corresponds to the id of the object, mirroring the value found in the exported configuration or obtained from the REST API.



- **Search Mechanism:** The search mechanism operates in two steps: finding matching results and navigating to the matched result. However, note that navigating to the matched result might not be supported for complex custom components or specific corner case paths.
- **Non-Editing Functionality:** The Search tool functions solely to display results and does not facilitate inline editing of parameter values.

## Manage and use test sessions

When you create a new test, LoadCore establishes a *test session* which remains available until such time as you decide to delete it (if ever). This way, you can access existing test configurations to change the settings and to view details, or to re-run a test session.

### Chapter contents:

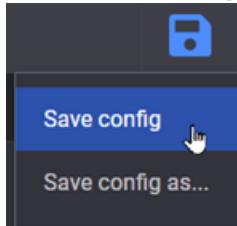
<b>Save test sessions</b>	41
<b>Manage test sessions</b>	41
<b>Import and export sessions</b>	44
<b>Delete configs and sessions</b>	45

## Save test sessions

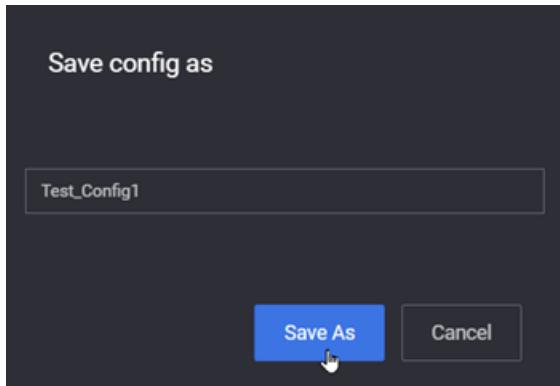
Once a test is configured, you can record its configuration as a session, edit and save it for future use.

To save a configuration file, do the following:

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

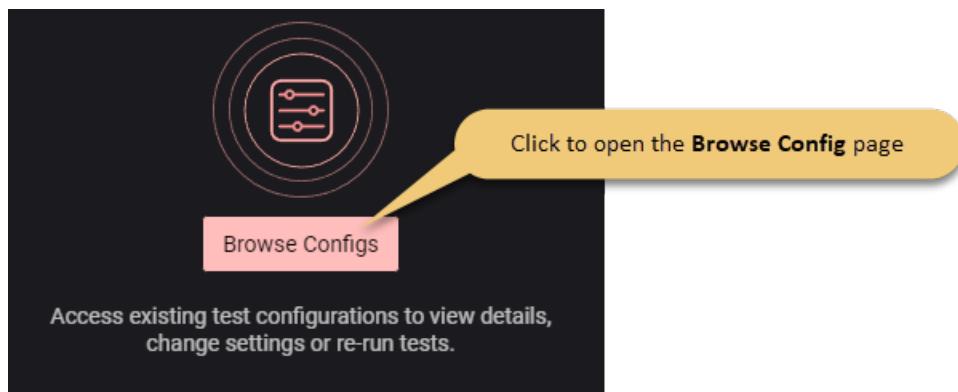


3. Click **Save config as** to save your test configuration with a specific name.
4. Provide the name for the test configuration in the **Save config as** window and click the **Save as** button.



## Manage test sessions

Managing saved tests is done on the **Browse Configs** page. To access the page, click the **Browse Configs** button from the main LoadCore Dashboard.



The **Recent Configs** list contains default configurations plus previously loaded configurations. If you select one of the configurations (by clicking it) a new session is created with this configuration loaded inside of it.

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

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

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

## View configuration categories

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



## Manage configurations

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

1	Config Name	2	Public	3	Created	4	Last modified	5	Application	6	Config Type	7	Owner
8	<input type="checkbox"/> Full Core New	<input checked="" type="checkbox"/>	Mar 19, 2025, 3:52:02 PM	Mar 19, 2025, 3:52:02 PM	Full Core	admin@example.org							
9	<input type="checkbox"/> Full Core Base Config	<input type="checkbox"/>	Feb 14, 2025, 10:51:04 AM	Mar 19, 2025, 3:51:42 PM	Full Core	system							
10	<input type="button" value="Delete"/>	<input type="button" value="Export"/>	Items per page: 15 ▾ 1 – 15 of 298   < < > >										

1	Details on the test name.
2	A selectable check-box indicates the test can be shared as public, a lock symbol shows that the configuration is locked for sharing (applicable on system or linked resource configurations). See <a href="#">Sharing configurations between users</a> for more information.

3	Timestamp of the creation date.
4	Timestamp of the last modification.
5	Indicates the test type.
6	Indicates the test owner.
7	Click the name link. You can open the current session from here, or create a new session based on this configuration.
8	Use to select a test configuration.
9	Indicates a base configuration <b>NOTE</b> For the base configurations, the test owner is <i>system</i> .
10	Click the button to delete the test configuration.
11	Click the button to export the test configuration.

## Sharing configurations between users

Private configurations can be enabled for public sharing with other middleware users.

To make a private configuration public:

1. Create a new or select an existing configuration (created by the current user).
2. From the **Public** column, select the check-box.

**IMPORTANT** Only the original creator can make the configuration public.

3. The configuration is now public, and:
  - all users in the MW will be able to see the configuration, and can load it into a new session.
  - the configuration can be deleted/modified only by the original creator.
  - another user cannot overwrite the public configuration.
  - when loaded into a session by a different user, the respective user can only save a new private configuration from the respective session.
  - when handled by a different user, if a public configuration is selected along other private configs with the intent of deletion, the Delete action becomes unavailable (only Export option can be used).

## Import and export sessions

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

If you want to export only a specific configuration, select it from the configuration list and select **Export**.

### Import test configurations

To import a saved test configuration from disk, do the following:

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

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

Config Name	Last accessed	Application	Config Type	Owner
Full Core New (copy from May 11 10:03:44)	May 11, 2023, 1:03:44 PM	Full Core	admin@example.org	
Full Core New	May 11, 2023, 12:55:29 PM	Full Core	admin@example.org	
Full Core Base Config	The name of the test when it was imported for the first time.	Full Core	system	

#### NOTE

By default, when you import a new test, the displayed name is the name you have in the JSON file under `displayName` - in this case, the `displayName` is Full Core Base Config. The second time it is imported, the test name is concatenated with `<date> <time>`.

## Export a saved test configuration

To export a saved configuration, do the following:

1. From the **Dashboard** page, click the **Browse Configs** button. The **Browse Configs** page appears.
2. From the **Test Categories** section, select the category containing the test to be downloaded.
3. Select the test configuration you want to download and click the **Export** button. When in tile view mode, click the **Download** button from the test tile.
4. Specify the download file name and select the download location.
5. Click **OK** to download the test configuration.

#### NOTE

The configuration file is exported as a JSON file.

## Delete configs and sessions

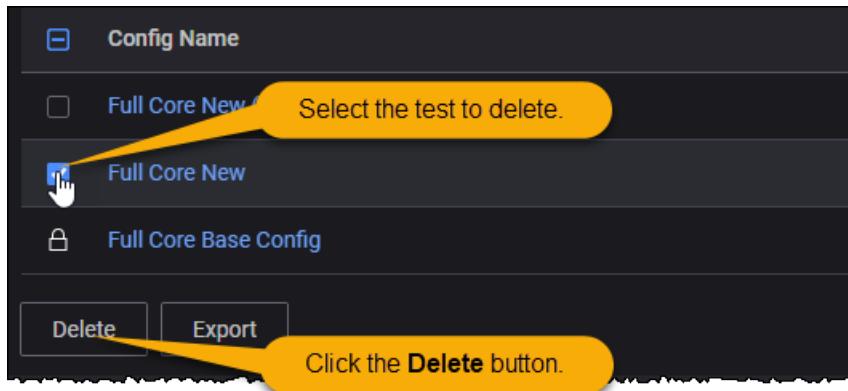
The terms *test config* and *test session* are not entirely synonymous. A "config" refers to a configuration definition file (JSON format), whereas a "session" is an instance of that file that is loaded in memory and is capable of being run.

### How to delete a LoadCore config

To delete a saved configuration from the **Browse Configs** page, do the following:

1. From the **Dashboard** page, click the **Browse Configs** button. The **Browse Configs** page appears.

2. From the **Test Categories** section, select the category containing the test to be deleted.
3. Select the test configuration you want to delete and click the **Delete** button.



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

### Important notes

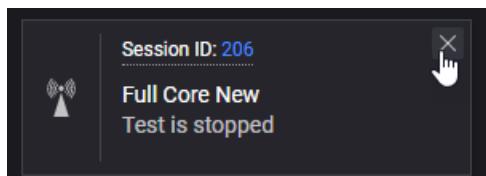
Before deleting a session, be aware of the following application behaviors:

- The session will be permanently removed and cannot be recovered.
- However, when you delete a session, the session's config is not deleted. Therefore, you can create new sessions based on that config.
- If you have a session open, and you delete the config upon which the session is based, the session is not deleted. Therefore, you can open the session and save a new config from it.

### How to delete a Keysight Open RAN Simulators, Cloud Edition 5.1 session

You can also delete a test session from the Dashboard:

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



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

## Upgrade the MiddleWare VM

To upgrade the LoadCore MiddleWare VM, do the following:

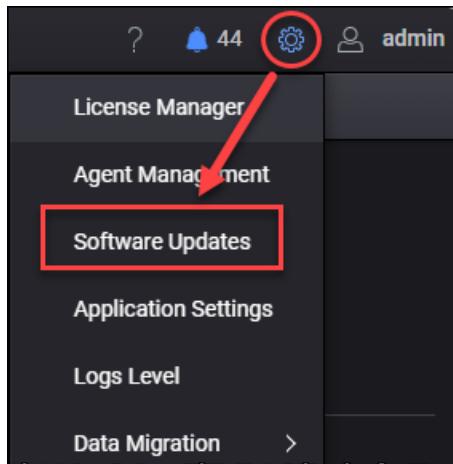
1. Download the latest upgrade file from LoadCore dedicated section on Keysight Software Manager:

<https://ksm.software.keysight.com>

NOTE

You will need to login with the account for which the licenses have been assigned/generated.

2. Before initiating the upgrade, make sure all the sessions are closed and the configs have been exported.
3. From the Settings Menu (⚙️), select **Software Updates**.



4. Use the **Select packages for upload** button to choose the file that was downloaded at [step 1](#).

A screenshot of the Software Updates page. The top navigation bar shows "Home > Software Updates". The main area is divided into two sections: "Installed Software:" and "Ready to be installed:". The "Installed Software:" section lists several packages with their versions:

Installed Software	Version
ATI Update	KCOS Framework
23.4.4	0.38.3
KCOS Host System	KCOS Keycloak Operator CRDs
0.33.5	17.0.0-ks0.4.16
KCOS local storage	KCOS SSO
0.38.3	0.15.28
Keysight Open RAN Simulators, Keysight Nimbus Mosaic Cloud Edition	
4.2.0-3747-346	0.1.0
Keysight NimbusMosaic	WAP
0.9.33-23-1	1.0.11483+releaseloadcore42

The "Ready to be installed" section says "There is no software ready to be installed." A red box highlights the "Select packages for upload" button at the bottom left of the "Installed Software" section, and another red box highlights the "Start update" button at the bottom right.

Wait for the upload to finish. The new version will show highlighted in green on the right. Select **Start update**.

**NOTE**

The upgrade process can take up to 30 minutes. It is recommended that the Middleware should not be used during this time.

Alternatively the upgrade can be done from the command line (after following [step 1](#) and [step 2](#)):

3. Copy the previously downloaded upgrade file (for example, `LoadCore-MDW-4.3.0-1310-459.tar`) to the home folder `/home/admin`.

4. To start the upgrade process run the command:

```
kcos deployment offline-install MDW-xxx-xxxx-xxx.tar (replace with the appropriate  
version)
```

For this example, the command is:

```
kcos deployment offline-install MDW-4.3.0-1310-459.tar
```

# 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

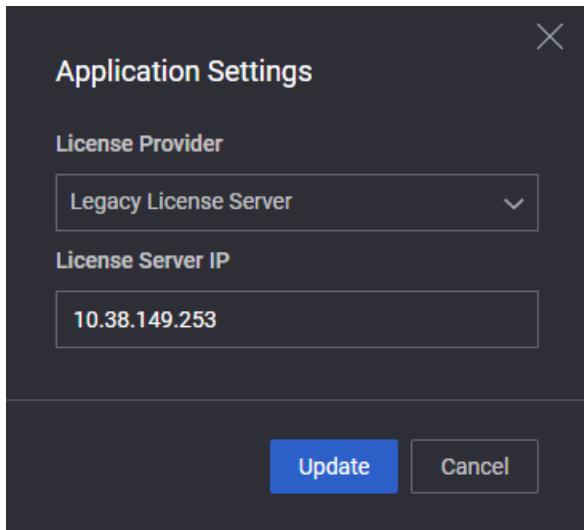
This section displays info related to the current installed software version of LoadCore.

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).

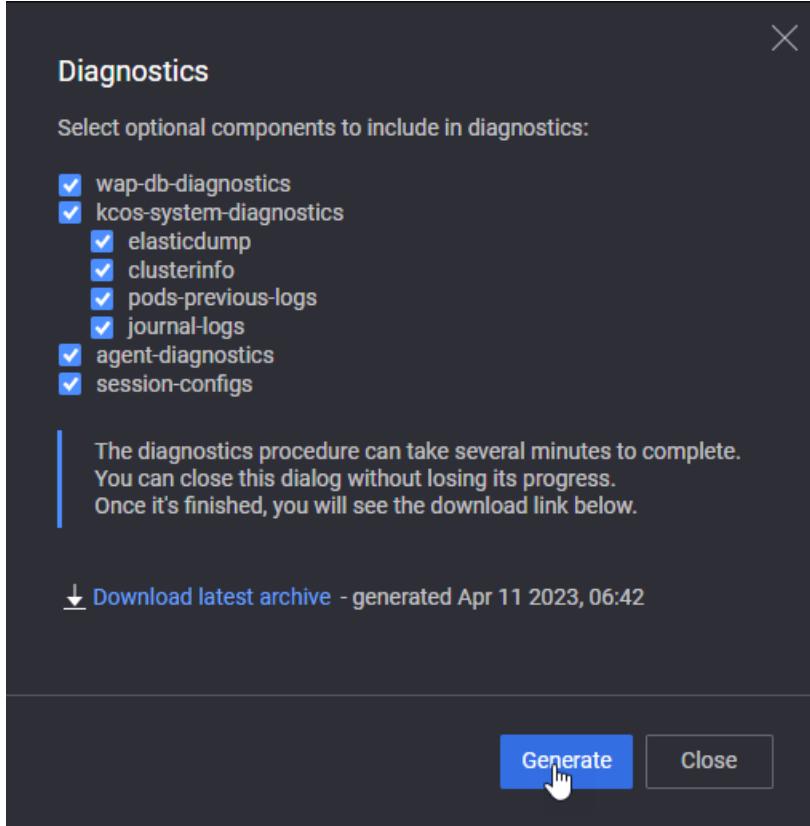
- **External License Server** - select this option to set an external license server (using the new LicenseManager 1.7 available with the LoadCore 3.2 release).
- **Embedded License Server** - the license server that is included in LoadCore MW.

## Collect Diagnostics

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

To collect diagnostics, do the following:

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



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

## Collect Logs

To collect logs info, do the following:

1. Click on **Logs Level** in the **Settings** menu. The Controller Logs Level window appears.
2. Select the log level used to collect diagnostics. Available options are:

- **ERROR**- Designates messages indicating that an error has occurred that impacts application stability.
  - **WARN** - Designates messages indicating that an error has occurred that potentially impacts application stability.
  - **INFO** - Designates informational messages that highlight the progress of the application at coarse-grained level.
  - **DEBUG** - Designates fine-grained informational events that are most useful for debugging the application.
4. Click **Generate**. The diagnostics procedure can take several minutes to complete. Once it is finished, a download link will be displayed.
  5. Select the download link in order to retrieve the diagnostics report.

## System Monitor

LoadCore system monitor tool is used to check the controller health and review the used resources and their availability. Also, it allows to perform a system cleanup:

1. Click on **System Monitor** in the **Settings** menu.
2. Select the required option:
  - **Controller Health** - this will open the Controller Health dashboard, where the available controller resources are displayed.
  - **System Cleanup** - this will open the System Cleanup window where the size of the following items are displayed: **Logs size**, **Diagnostics size**, **Migration size**. Use the **Delete** button to delete the archives.

## Data Migration

LoadCore data migration tool allows you to migrate controller data from one setup to another. You can export authentication data and other data (such as configurations, external license servers, controller proxies, and results) from a source controller, which you can then import to a new target controller. When the import procedure is complete, the resources that you imported from the source controller will have replaced all the existing data on the target controller.

**IMPORTANT** The export procedure cannot run when the available controller disk space is lower than 50%. To free up disk space by removing diagnostics, logs, or migration archives, use the **System cleanup** option under the **Settings** menu > **System Monitor**.

To export data from the source controller:

1. From the **Settings** menu, select **Data Migration** > **Export Controller**. The **Export Controller Data** window opens informing you of the components to be exported.
2. Click the **Start** button. A notification at the bottom of the screen informs you that the migration package is being queued in preparation for export, and the **Export Controller Data** will automatically close.

When all the export resources are collected and available on your local system, a notification informs you that the export package was created.

The export package is downloaded on your local system in the form of a compressed .zip file, under your usual downloads location (for example, C:\Users\<user name>\Downloads\migrate\_package1676028828)

To import data on the target controller:

1. From the **Settings** menu, select **Data Migration > Import Controller**.  
The **Import Controller Data** window opens.
2. Click **Select migrate package for upload**, and select the migration package that you exported from the source controller, and click **Open**.  
A warning is displayed informing you that the import procedure cannot be canceled or reverted after it is initiated.
3. Confirm acknowledgment of data loss by selecting the **I understand this will wipe existing data** check box.
4. Click the **Start** button.  
The import procedure initiates. The application screen is grayed out during import and will become active again when the import procedure is complete.
5. After the import procedure is finished, close the **Import Controller Data** window.
6. Log out of the web UI, and log in again to see the newly imported controller data.

## 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.

# Work with Statistics

The **Statistics** page has several panels, which can be dragged and dropped and rearranged on the dashboard. They can also be duplicated or removed, and there are a wide variety of formatting options for each panel.

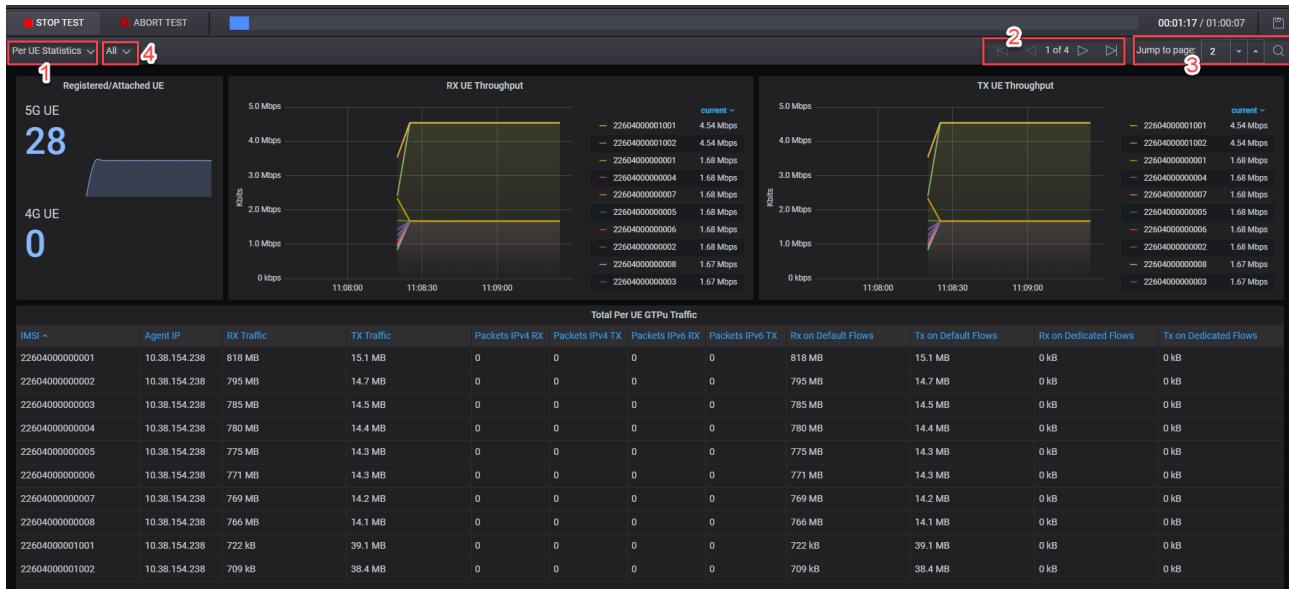
### NOTE

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

## Filter Per UE Statistics

Select the drop-down menu (1) on the top left and switch between **Global Statistics** to **Per UE statistics**.

By default the UEs will be displayed in IMSI ascending order and will be split in pages of 10 each:



The arrow buttons (**2**) on the upper right can be used to switch between pages, one by one.

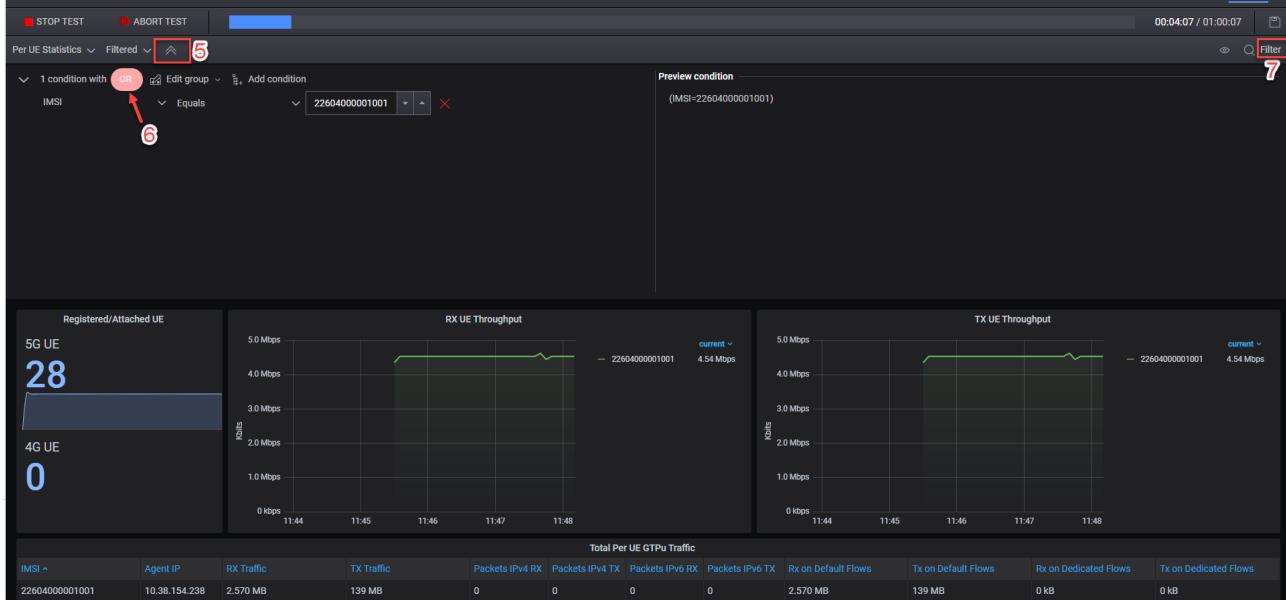
Type in a number in the **Jump to page** field (**3**) and then click the magnifying glass button to jump directly to the chosen page.

Expand the **All** drop-down menu (**4**) and select **Filtered**. To view and change the filter conditions click on the switch button (**5**).

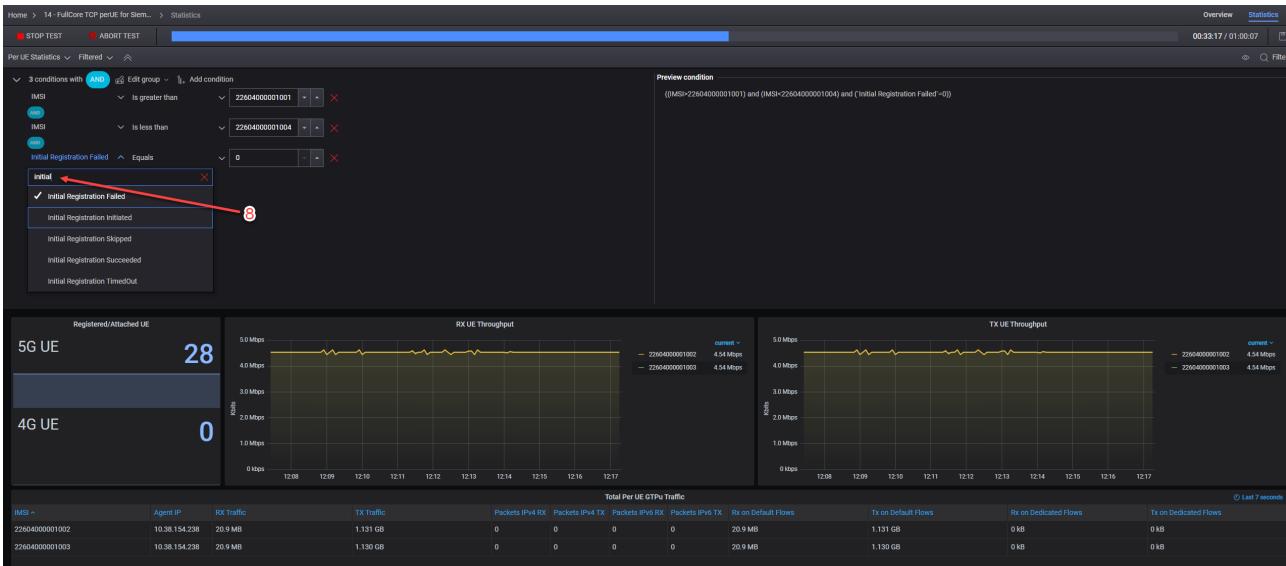
You can add multiple groups and conditions. You can change the operator from **AND** to **OR** by clicking on the respective button (**6**).

Select the **Filter** button (**7**) on the top right to apply the chosen parameters. Wait a few seconds for the filter to take effect.

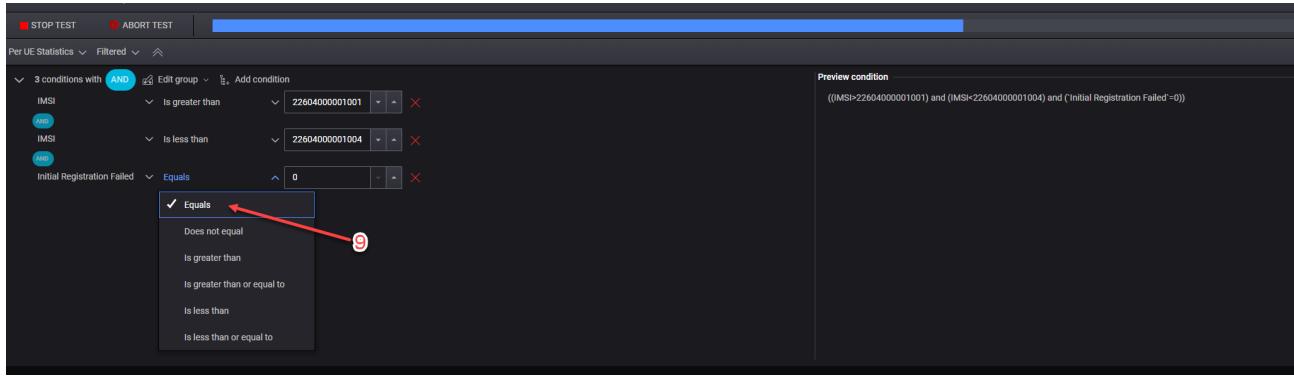
**NOTE** After a filter is applied, only the first 10 results are displayed (even though the filtered data produce more than 10 results).



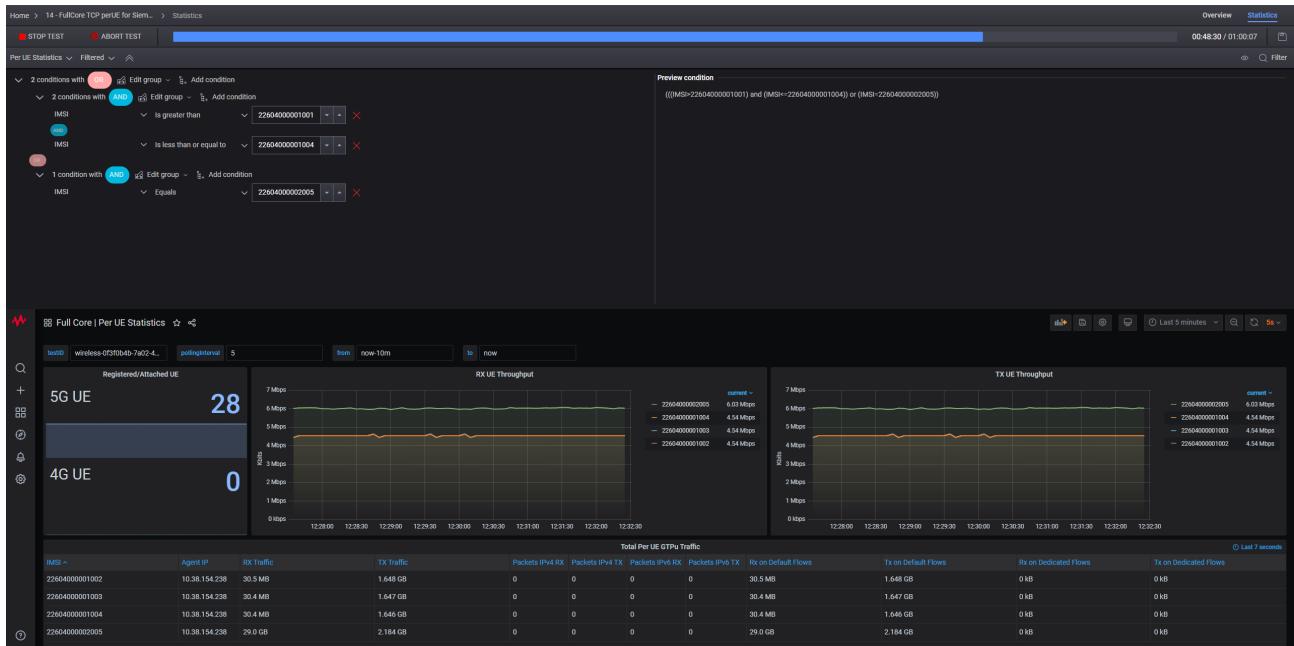
It can be searched and applied a condition for every per UE statistic (8) that is generated in the test: IMSI, IP, registration success/failed, N2 handover, number of bytes or packets, NSSAIs, etc.



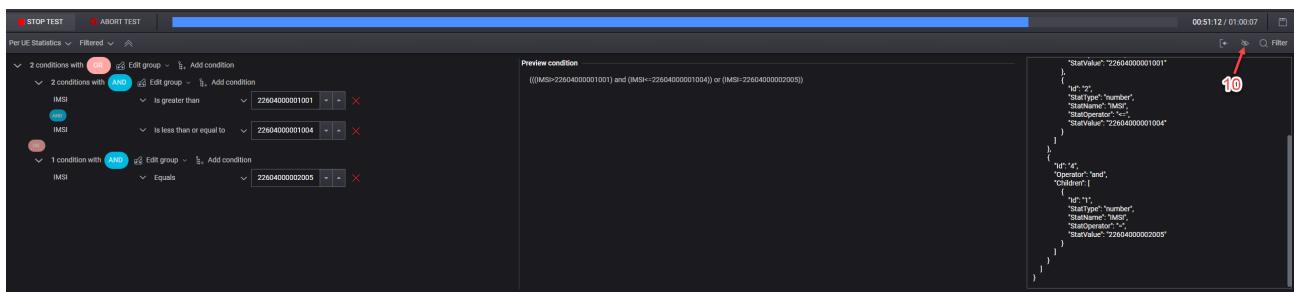
The relational operator (9) can also be changed as needed.



If the **AND/OR** button is clicked, it will change for all conditions in the group, so groups are needed for different logical operators. In the below image there is one group with just one IMSI and another group with 2 IMSI conditions.



The filter conditions can also be seen and changed from its respective json, by clicking the eye button (**10**). This can also be used to copy/paste a filter from a different test.



## Filter Per PDU Statistics

Select the the drop-down menu (1) on the top left and switch between **Global Statistics** to **Per PDU Statistics**.

By default on each page there are showed first in IMSI order and then in PDU order the first 10 results. For example, below it displays the first 5 IMSIs, each having 2 PDUs:

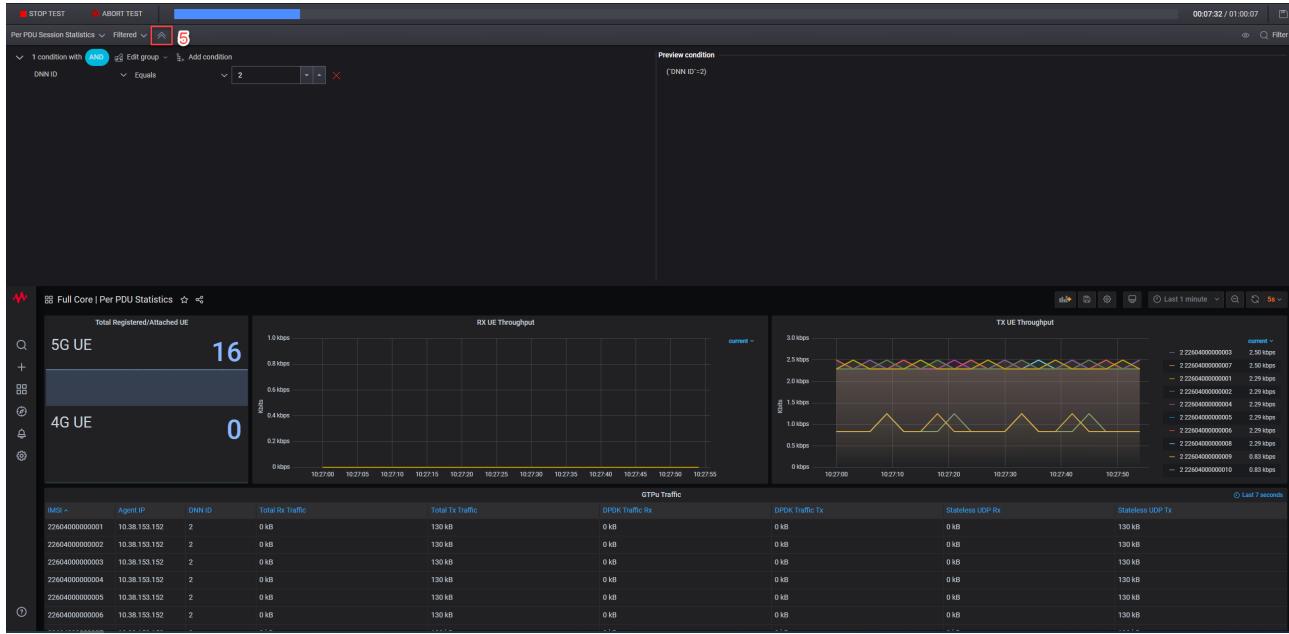


Same as in per UE statistics, the arrow buttons (2) on the upper right can be used to switch between pages, one by one.

Type in a number in the **Jump to page** field (3) and then click the magnifying glass button to jump directly to the chosen page.

Expand the **All** drop-down menu (4) and select **Filtered**. To view and change the filter conditions click on the switch button (5).

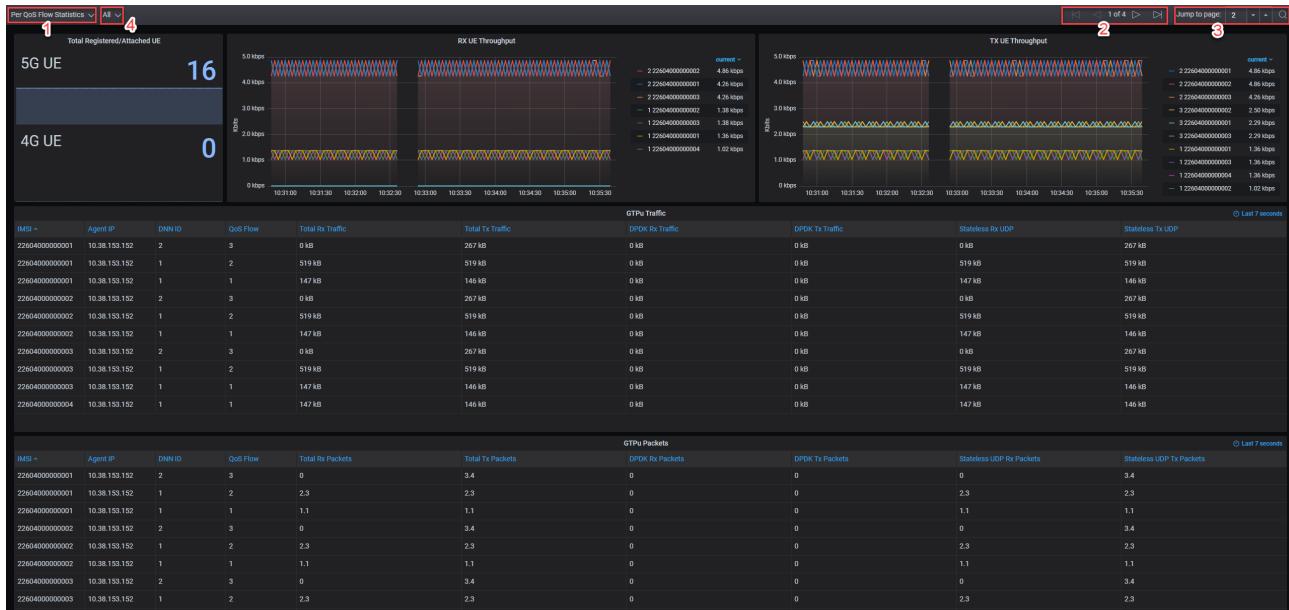
Filtering works the same as in Per UE statistics, only the conditions/statistics that can be selected are slightly different. Below it was filtered only by DNN 2, which does only uplink traffic:



## Filter Per QoS Statistics

Select the drop-down menu (1) on the top left and switch between **Global Statistics** to **Per QoS Statistics**.

By default on each page there are showed first in IMSI order and then in QoS order the first 10 results. For example, below it displays the first 3 IMSIs each with 3 QoS flows and then the 4th IMSI with its 1st QoS flow. Only the 1st and 2nd QoS flow are used for downlink traffic:

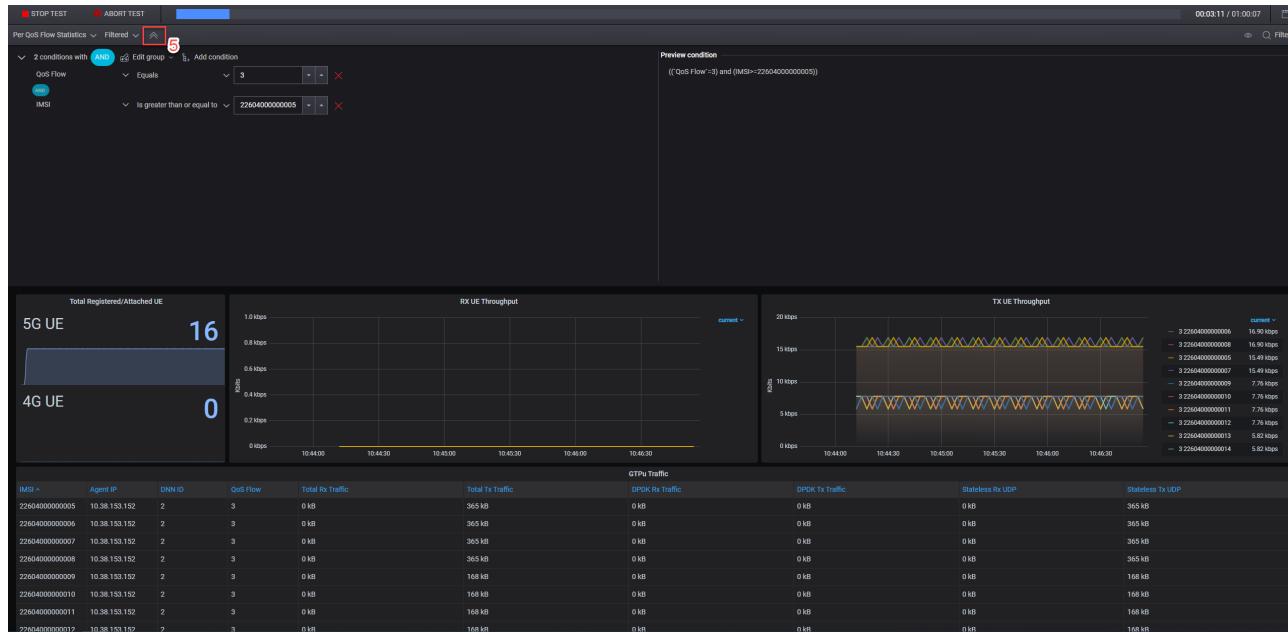


Same as in per UE and per PDU statistics, the arrow buttons (2) on the upper right can be used to switch between pages, one by one.

Type in a number in the **Jump to page** field (**3**) and then click the magnifying glass button to jump directly to the chosen page.

Expand the **All** drop-down menu (**4**) and select **Filtered**. To view and change the filter conditions click on the switch button (**5**).

Filtering works the same as in Per UE and per PDU statistics, only the conditions/statistics that can be selected are slightly different. Below it was filtered by QoS flow 3, and IMSI:



## Debug

LoadCore offers support for debugging capabilities.

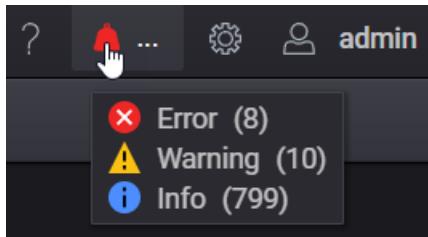
In this section:

<b>View Notifications and Test Events</b>	<b>58</b>
<b>Manage Test Results</b>	<b>60</b>
<b>Troubleshooting</b>	<b>61</b>

## View Notifications and Test Events

The navigation bar displays a notifications icon and a counter showing the total number of triggered notifications since the counter was last reset for the current LoadCore instance. 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.

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



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

#### Types of events:

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

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

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

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

Here you can view details on the registered events regarding the logging date, their severity type and description. You can choose to display all events or certain types of events, based on their severity, by selecting or clearing the associated check-box.

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

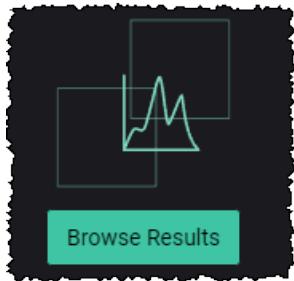
The screenshot shows the 'Events' page with a header 'Home > Events'. Below the header is a section titled 'Filter events by' with three main categories: 'Message', 'Date', and 'Notification type'. Under 'Message', there is a search bar 'Type keywords' and a magnifying glass icon. Under 'Date', there are two date pickers labeled 'From' and 'To', with a calendar icon between them. Under 'Notification type', there are four checkboxes: 'All' (checked), 'Info' (checked), 'Warning' (unchecked), and 'Error' (checked). Below the filter section is a table with columns 'Date', 'Type', and 'Message'. The table contains five rows of log entries:

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

## 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.

**NOTE**

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

- Delete the test results, by selecting the **Delete** button.

**NOTE**

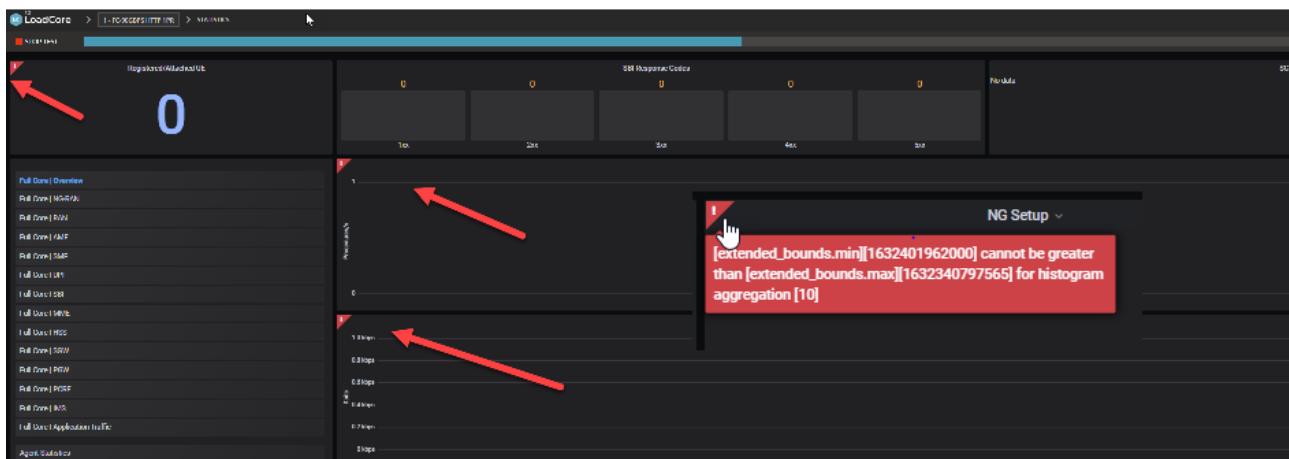
At this moment, LoadCore does not have an automatic mechanism to delete old results, therefore this operation must be done manually in order to prevent MW disk to become full (especially running long duration tests).

## Troubleshooting

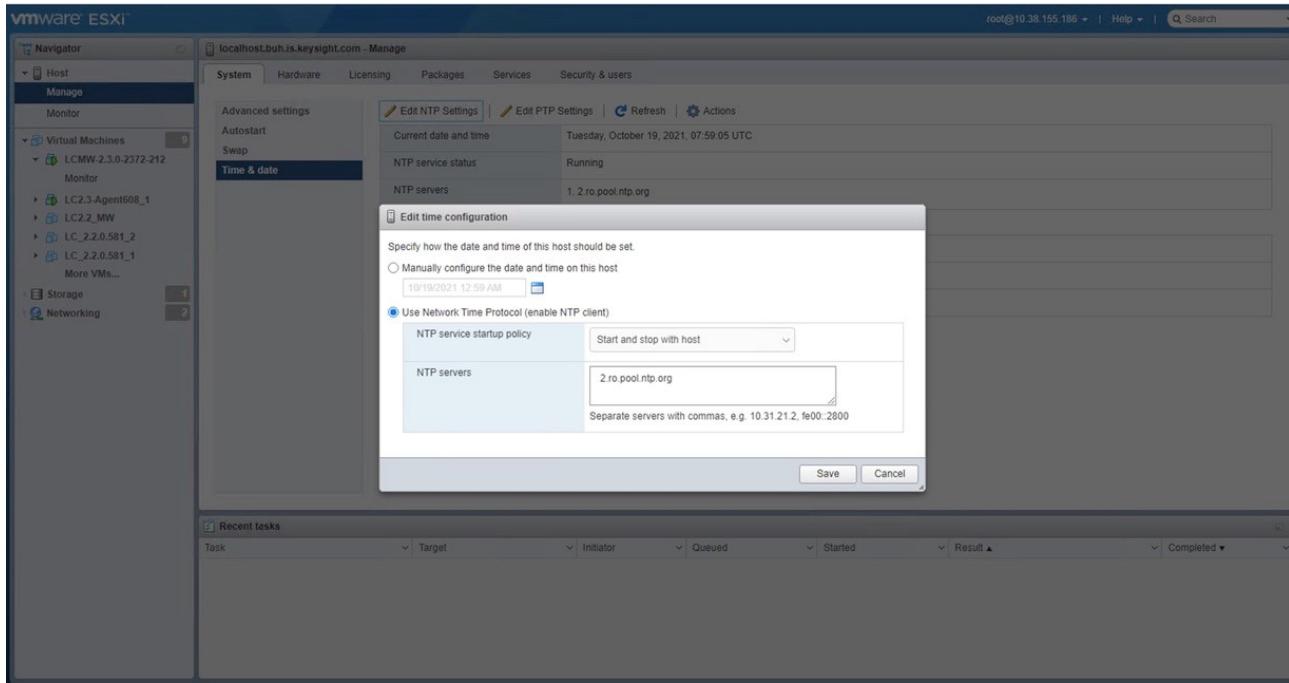
This section presents the most common errors or issues and their associated resolution (if available).

### 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](http://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.

**CHAPTER 4**

## **Assign and manage agents**

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

**Chapter contents:**

<b>About traffic agents</b> .....	<b>63</b>
<b>Assigning agents to nodes</b> .....	<b>63</b>
<b>Agent management</b> .....	<b>65</b>
<b>Network Management</b> .....	<b>68</b>
<b>Distribution Mode feature</b> .....	<b>69</b>

## **About traffic agents**

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

Tags provide a flexible and simple method of assigning metadata to agents. There are two types of tags:

Type	Color	Description
System tag	Blue	These tags are defined by LoadCore. You can hover over the system tag icon to display the tag information.
User-defined tags	Gray	You can add custom tags from the Agent Management window. These are tags that you create; they are free-form, which gives you the ability to categorize or mark agents in any way that supports your test requirements. Refer to <a href="#">Agent management on page 65</a> for instructions.

## **Assigning agents to nodes**

You cannot run a LoadCore test until you have assigned agents to all of the test nodes. To assign an agent to a node:

1. In the topology window, select the traffic agent icon on the top right corner of the node.  
The icon that represents the agent can be any of the following:



— No agents are assigned to the node.



— One or more agents are assigned.

LoadCore opens the **Agents Assignment** window, which presents a list of agents. If the list has no filters set, then all agents are listed.

2. Assign specific agents or all available agents to the node:

- To assign specific agents (one or more) to the node, select the check box next to the agent's IP address.
- To assign all available agents to the node, select the **Select Agent** check box (located in the table header).

Note that you can display the agent ID by hovering over the IP address.

### Agent Assignments window

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

Column	Description
Owner	<p>Hover over the <b>Owner</b> icon to see the current agent ownership and status, which will be one of the following:</p> <ul style="list-style-type: none"> <li>• The agent is owned by the user whose email address is listed. In this case, the agent is not available for assignment.</li> <li>• The agent is offline. In this case, the agent is not available for assignment.</li> <li>• The agent is available for assignment.</li> </ul>
Select Agent	<p>Use the check box next to the IP address to select that agent for assignment. You can also select all available agents by selecting the <b>Select Agent</b> check box (in the table header).</p>
Tags	<p>This column displays the tags associated with each agent. Each tag indicates the number of agents to which it is associated.</p> <p>Refer to <a href="#">About traffic agents</a> for more information about tags.</p>
Hostname	Displays the hostname.
UPF Ranges	<p><b>IMPORTANT</b> This option is available only for <a href="#">Full Core topology &gt; UPF Ranges</a>. If enabled, it allows the selection of simulated UPF ranges for the selected agent.</p>
Connections	<p>The table displays the available interface and the MAC address for each wireless connection. The interface can be selected from the drop-down list.</p> <p><b>NOTE</b> For the LoadCore nodes that have multiple interfaces, for each interface, you can change the interface type using the drill-down option.</p>

### Quick Interface Mapping

The Quick Interface Mapping table allows you to easily assign multiple interfaces to multiple agents. First, select two or more agents to set, then decide over the next **Action**:

Setting	Description
Action	<p>There are two actions available:</p> <ul style="list-style-type: none"> <li>• <b>Set</b> - select an Agent Device and one or multiple Agent IPs as Source, while selecting the desired interfaces as Destination.</li> <li>• <b>Copy</b> - select as one or more interfaces and one Agent IP as Source, and one or more Agents as Destination.</li> </ul> <p>Depending on the action selected, the rest of the table headers will change to meet the rules.</p>
<i>Set configuration:</i>	
Device	List the devices available for the filtered and enabled Agents.
Destination	<p>Includes two expandable lists:</p> <ul style="list-style-type: none"> <li>• <b>Interfaces</b> - expand to see the selectable list of Interfaces available on all nodes. You can select one, more or All interfaces, depending on your configuration needs.</li> <li>• <b>IPs</b> - expand to see and select the IPs applicable for your interface selection. Note that in this case you can select more than one IP.</li> </ul>
<i>Copy configuration:</i>	
Source	<p>Includes two expandable lists:</p> <ul style="list-style-type: none"> <li>• <b>Interfaces</b> - expand to see the selectable list of Interfaces available on all nodes. You can select one, more or All interfaces, depending on your configuration needs.</li> <li>• <b>IP</b> - selected by default, it will show only the IPs applicable for your interface selection. Note that in this case you can select only one IP.</li> </ul>
Destination	Shows the list of all filtered and enabled Agents' IPs that can be selected for this setup.
Map Interfaces button	Hover over this button for a short summary of your selection. Click to apply the best effort action.

Once these settings done, click on **Map Interfaces** to apply changes, and then press the **Apply** or **Apply & Close** buttons to save the configurations.

## Agent management

You manage your LoadCore agents from the **Agent Management** window, which is accessed from the Setting menu (⚙). This window displays detailed information for all or selected agents and provides all of the functionality needed to manage them.

- [Agent Management window on the next page](#)
- [Selecting agents on the next page](#)

- [Search, select, and filter agent data on the facing page](#)
- [Adding and removing tags on the facing page](#)
- [Agent management actions on the facing page](#)

## Agent Management window

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

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

## Selecting agents

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

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

## Search, select, and filter agent data

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

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

## Adding and removing tags

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

### Add a custom tag:

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

### Remove a tag:

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

## Agent management actions

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

Function	Description
Clear ownership	Releases your ownership of the selected agents.
Hard reboot	Performs a hard reboot on the agent (the agent machine is power-cycled).
Soft reboot	Performs a soft reboot on the agent (the agent system restarts without a power cycle).
Update	Performs the update of the Traffic Agent version with a package update of your choice (a TGZ archive). This button is enabled when at least one agent is selected.
Delete	Removes the selected agent(s) from the Agent Management list.

## Network Management

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

### Table description

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

Column	Description
Order	This option allows you to select the agent distribution order when running with multiple agents on the same node (when you are not using a switch to connect all agents).
Agent	Displays the agent's IP address. When hovering over the IP address of the agent, the agent ID is displayed.
Tags	This column displays the tags associated to each agent.
Impairment profile	Allows you to select an impairment profile from the drop-down list.
Agent Interface	Displays the agent's interface Name and MAC address.
Network Stack	<p>This option allows you to select the network stack used to run the test:</p> <ul style="list-style-type: none"> <li>• <b>Linux Stack</b></li> <li>• <b>IxStack over Raw Sockets</b></li> <li>• <b>IxStack over DPDK</b></li> </ul> <p>An agent compatible with IxStack is marked using an <code>IxStack: On/Off</code> system tag.</p>
SRIoV	This option is disabled when <i>Network Stack</i> is set to Linux Stack. For IxStack over

Column	Description
	Raw Sockets or IxStack over DPDK, this option is enabled based on the selection (it can be enabled or disabled based on your agent's configuration).
Traffic Capture	<p>This option allows you to enable or disable traffic capture on all or specific interfaces, based on your test configuration. This option can be used while a test is running.</p> <p>If the test was started with the capture disabled, you can enable the capture during the test. After enabling the capture, you must select <b>Apply</b> for the changes to take effect. The capture can be downloaded using the <a href="#">Download Capture</a> button. To stop the capture, you must disable the traffic capture (using the toggle button) and then select <b>Apply</b>.</p> <p>Also, if the test was started with the traffic capture enabled, the capture can be stopped while the test is running.</p>
Download Capture	Select to download the traffic capture. Capture needs to be stopped first (see Traffic Capture) before downloading. After it has been downloaded, capture can be resumed.
Entity	Displays the nodes on which the agent has been assigned. When hovering over the node, it displays the node's interface names.

**IMPORTANT**

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

## Filtering agents

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

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

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

## Distribution Mode feature

### Distribution Modes for Nodes

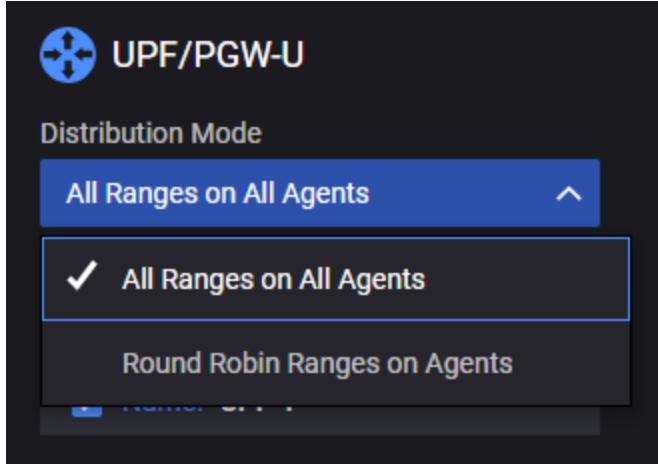
For convenience, you are now able to see or select (if available), the way node ranges are distributed on agents. The **Distribution Mode** parameter is available even if no agents are assigned, but its value can change when assigning multiple agents and/or when adding multiple ranges.

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

Distribution Mode	Description/Example
All Ranges on All Agents	All ranges will be distributed on all agents and the IP addresses will

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

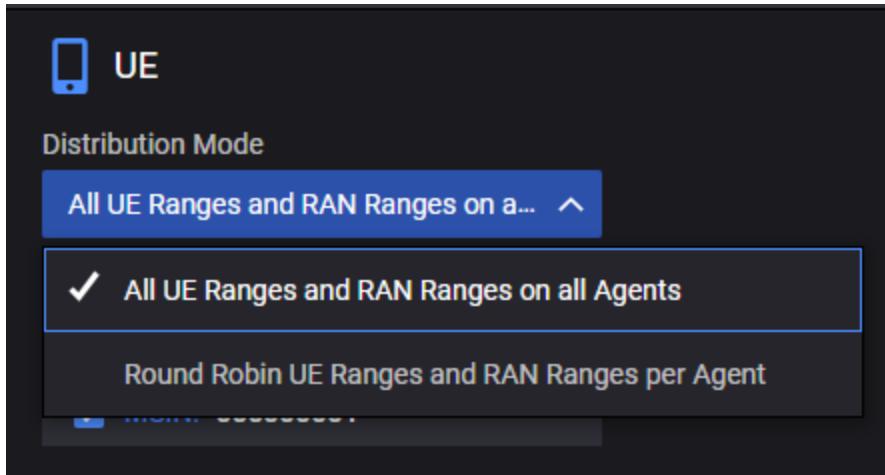
For more details, refer to each node for the available distribution mode.



### UE-RAN Distribution Modes (configurable on UE box)

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

Distribution Mode	Description/Example
<b>All UE Ranges and RAN Ranges on All Agents</b>	For example, for a test with 2 agents and 2 UE ranges and 2 RAN ranges: <ul style="list-style-type: none"><li>UE range1 and UE range2 and their parent ranges as well as all RAN ranges part of Mobility Path and Secondary RAN ranges will be distributed to both agent1 and agent2</li></ul>
<b>Round Robin UE Ranges and RAN Ranges per Agent</b>	For example, if UE range1 is distributed to agent1, parent RAN range as well as all RAN ranges part of the Mobility Path (visited gNB/eNB ranges), and the Secondary RAN ranges will also be distributed on agent1.



This page intentionally left blank.

**CHAPTER 5**

## **Work with the Resource Library**

---

LoadCore allows you to view, import and export various resources such as payloads, TLS certificates, TLS keys, TLS DHS, playlists, media files, captures and custom applications. You can access the Resource Library from the **Settings** (⚙) menu > **Library** > **Resource Library**.

See the following sections for details on how to:

<b>Import Captures</b> .....	<b>73</b>
<b>Create Custom Applications from Imported Captures</b> .....	<b>74</b>
<b>Edit Custom Applications</b> .....	<b>75</b>
<b>Export Custom Applications</b> .....	<b>76</b>
<b>Import Custom Applications</b> .....	<b>76</b>
<b>Procedures Resources (SIP/Media/Flow)</b> .....	<b>77</b>
<b>Custom Fuzzing Scripts</b> .....	<b>108</b>
<b>Export Other Resources</b> .....	<b>108</b>
<b>Import Resources</b> .....	<b>108</b>

## **Import Captures**

You can import and view available captures from the **Settings** (⚙) menu > **Library** > **Resource Library**. You can use imported captures to create custom applications from the LoadCore UI. The PCAP or PCAPNG file formats can be used for importing operations.

The following limitations apply when importing captures:

- Capture files must include at least one TCP flow or one UDP flow.
- The maximum capture size is 1 GB.
- The maximum number of flows per capture is 10,000 (with one exchange per flow).
- The total number of exchanges per capture is 10,000.

To import a packet capture:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library** > **Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select **Captures**.

If no captures have been imported yet, the page will be blank. If capture files have previously been imported, they will be listed on the page with a capture ID and a file name. To view more details about each capture, expand each entry by clicking the **Expand** (▶) button. You can view each flow ID, source and destination addresses, source and destination ports, transport protocol, available exchanges for each flow, including the first 1024 bytes of payload for each direction of the exchange.

4. Click **Import** in the left bottom corner of the screen.
5. Browse to the capture file you want to import and select it. Then click **Open**.  
After the capture file is uploaded, it will be displayed on the list of available capture files. The time it takes to upload the capture depends on its complexity. For example, a higher number of exchanges or smaller average payload sizes will increase the upload time.  
You can also delete an existing capture by selecting the capture on the list and clicking **Delete**.

See also [Create Custom Applications](#).

## Create Custom Applications from Imported Captures

After you import a capture, you can create a new custom application that you can use in your LoadCore tests.

An application can have multiple actions and one action can be created from:

- one full capture,
- a subset of flows from one or multiple captures, or
- a subset of exchanges from one or more flows and from one or multiple captures.

After the application is created it will be available in the list of applications just as the pre-canned applications.

The following limitations apply for creating custom applications from imported captures:

- HTTP transport protocol is not supported.
- Custom applications on ports 80 or 443 cannot be mixed with pre-canned web applications.
- Importing invalid packet captures will return an error message.
- Importing packet captures with unsupported IP protocols will return an error message.
- The UI displays only the first 1024 bytes of each client-to-server (C2S) and server-to-client (S2C) payload; however, the full payload size is visible.
- The total number of flows (connections) in a single application cannot be bigger than 64.
- The total number of parameters cannot be bigger than 10,000. The total number of parameters is equal to the sum of endpoints per action multiplied by the number of parameters per endpoint for the same action.

To create a custom application:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library > Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select **Captures**.  
The list of available captures opens. If no captures are displayed on the page, first [import a capture file](#).
4. Click **Create Apps** at the bottom of the screen. The Create App dialog opens.
5. Under each column on the Create App dialog, select the capture(s), flow(s) and exchanges(s) you want to use for the new application.

6. Then click the **Add**  button to add actions from the selected entries.
7. Click the **Create App** button in the bottom right corner of the dialog.  
The new application is created based on your selections and displayed under **Browse resources > Custom Applications** along with other pre-canned applications.

## Edit Custom Applications

After you create a new custom application, you can further customize it to fit the tests you want to run. After the application is created it will be available in the list of applications just as the pre-canned applications.

To edit a custom application:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library > Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select **Custom Applications**.  
The list of available custom applications opens. If no applications are displayed on the page, first [create a new custom application](#).
4. Click the **Expand** icon next to the application you want to edit. The available application actions are displayed.
5. To navigate between actions, flows, or exchanges, click through each action/ flow/ exchange fly-out panel.
6. To view the Client to Server and Server to Client payload, click the **C2S Payload** button or the **S2C Payload** button respectively.
7. To add a new action/ flow/ exchange:
  - a. Click the **Add**  button next to the component you want to add. The **Edit App** dialog opens, listing the available captures, the application name, and the already available actions/ flows/ exchanges for the current application.
  - b. Under **Select captures**, select the capture you want to use as the basis for your action/ flow/ exchange.
  - c. Then, under **Edit App**, click the **Add**  button under the action/ flow/ exchange list to add the selected capture as a new action/ flow/ exchange. The new component is added to the list under a default name which you can update by clicking the **Rename**  button and typing a new custom name for the action/ flow/ exchange.
  - d. You can also click the **Edit**  icon to update the selected action/ flow/ exchange. For example, when clicking **Edit**, you can see the list of flows and exchanges for an action and add new flows or exchanges by clicking **Add** .
  - e. To confirm all the changes and close the Edit App dialog, click the **Edit App** button in the lower right corner of the dialog. The new action/ flow/ exchange is displayed under the custom application.
8. To delete any action/ flow/ exchange, click the **Delete**  button next to the component you want to remove.

9. To change the order of actions/ exchanges, click and hold the **Reorder**  button. Then, drag and drop the item in the correct position.
10. To save all the changes you made for the selected custom application, click **Save App**.  
The changes are saved on the server, and when you enter a test session you will be able to add the application you edited to your test configurations.

## Export Custom Applications

After you import a capture and create a new custom application, you can export it from the LoadCore UI.

To export a custom application:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library > Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select **Custom applications**.  
The list of available custom applications opens. If no custom applications are displayed on the page, first [create a custom application](#).
4. Select the application you want to export.
5. Click **Export** at the bottom of the applications list. The selected application is downloaded on your machine as a .zip file. You can use this downloaded archive to import the same application on other LoadCore setups for example.  
You can also export multiple custom applications by clicking the **Export All** button under the **Browse resources** pane.

## Import Custom Applications

To import a custom application:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library > Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select **Custom applications**.  
The list of available applications opens.
4. Click **Import** under the **Browse resources** pane.
5. Browse to the application you want to import and select the .zip file. Then click **Open**.  
The custom application is loaded on the server and displayed under the list of **Custom Applications**.

## Procedures Resources (SIP/Media/Flow)

Resource Library holds all uploaded procedures listed under the **SIP Procedure**, **Media Library** and **Flow Procedures** sections. From **Settings** ( menu > **Library** > **Resource Library** > **SIP Procedure/Media Library/Flow Procedures** you can delete, export existing procedures, or import new procedures.

**IMPORTANT** The import can also be executed from the **Global Settings** section of each LoadCore configuration.

Procedures features:

- SIP includes procedures related to SIP signaling.
- Media includes procedures related to media (audio or/and video)
- Flow includes the Start and Stop procedures used to define an iteration. The number of iterations can be configured per each UE range on the Voice objective, Dial Plan section (a 0 meaning infinite loops).

The predefined procedures will be either available upon LoadCore installation, or delivered separately. If the latter, these procedures will have to be imported in the Resource Library.

Predefined procedures have to be pulled from the Resource Library, where predefined or user defined procedures are stored.

**IMPORTANT** These procedures are not shared with other user-accounts from the LoadCore machine.

The procedures from the Resource Library can also be exported individually, and then imported on the same or a different account/LoadCore VM.

Name	MD5	Size	Owner
Registration Subscribe waitNotify.json	4e9880efcf36f13116b9fa1d13750ff8-1	8055	admin@example.org
deReg-UnSub-waitNotify.json	bf9866e43562773a19f34e5c90b58b0-1	8097	admin@example.org
MO end call.json	01328b07a82a472c3539b4e9670fbff7-1	18261	admin@example.org
MT end call.json	582e980d3ce8425c4b0952eeda83b5a-1	2613	admin@example.org
MT IMS call setup.json	28fde0eb360d38d7859358c551ed3838-1	4358	admin@example.org
Registration.json	35af94f81002dff539cf099932b6e554-1	2569	admin@example.org
deRegistration.json	9357e69e537b8999f32e9f5943852e35-1	14626	admin@example.org
MO call setup.json	bddb301eebb38c5834cbca1a8c1872f-1	4706	admin@example.org
	2499f1918d76664127a539a896e2827f-1	4740	admin@example.org
	e1f8e229f7c4238be52148cd4da5edab-1	11103	admin@example.org

When importing a procedure or a configuration that contains procedures, a procedure detected to have the same name and/or content with an existing procedure will append a number to their name, to have a unique name for the imported JSON (for example, *Stop (1).json*).

## Procedures management

From Resource Library you can delete unused procedures. When deleting a procedure, if the selected one is used in a configuration or in a result, you will be prompted if you really want to delete the file. Select **Force Delete** go forward.

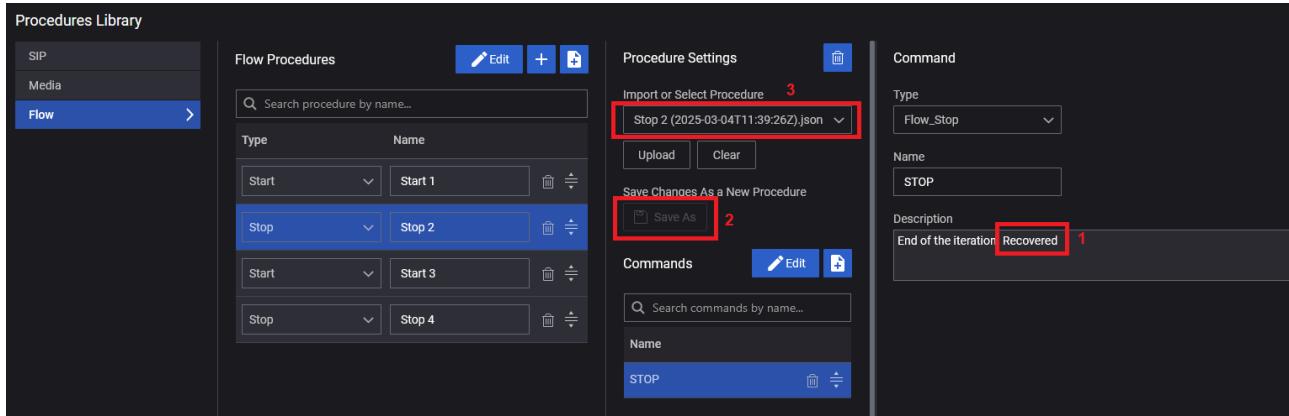
If a procedure that was actively used is deleted by accident, **Procedures Library** still preserves an entry available, along with a visible configuration, but procedure will not have a JSON file linked. If you want to run the configuration at this point, the following errors will show:

Jul 5, 2024, 4:44:27 PM	<span style="color: red;">✖</span> ERROR	Start operation aborted. Test stopped.
Jul 5, 2024, 4:44:24 PM	<span style="color: red;">✖</span> ERROR	Test stopped: Operation finished with error: Invalid payload received for file Stop (1).json
Jul 5, 2024, 4:44:24 PM	<span style="color: red;">✖</span> ERROR	Invalid payload received for file Stop (1).json
Jul 5, 2024, 4:44:23 PM	<span style="color: red;">✖</span> ERROR	Unable to find Flow Library File with id 20079
Jul 5, 2024, 4:44:22 PM	<span style="color: blue;">ℹ</span> INFO	Reserving 2 test agent(s)
Jul 5, 2024, 4:44:20 PM	<span style="color: red;">✖</span> ERROR	Unable to find Flow Library File with id 20079
Jul 5, 2024, 4:44:20 PM	<span style="color: red;">✖</span> ERROR	Unable to find Flow Library File with id 20078

To recover the procedure:

1. In the **Flow Procedures > Procedure Library**, identify the procedure that was saved under the respective name.
2. Observe that the procedure panel includes an empty field under the **Import or Select Procedure**, while the **Save As** button is disabled.
3. Select any of the **Commands** in the procedure and modify any field. The safest choice is to add/remove something from the **Description** field.
4. Press the **Save As** button.
5. The procedure is saved, and the **Import or Selected Procedure** field will show its new name and the new time stamp.

The test can now run with no errors.



## Procedures Library

Procedure Library includes predefined procedures pulled from the [Resource Library](#), or allows you to create new procedures.

### NOTE

When accessing the Procedures Library in a new test, there will be no procedures defined in it. The procedures can be either predefined, derived from the predefined procedures, or created from scratch.

**NOTE**

The resource library stores all predefined or user-defined procedures. These procedures are not shared with other user-accounts from the LoadCore machine.

This section describes how to:

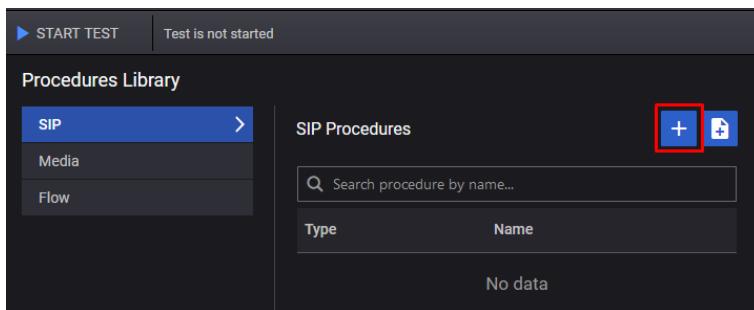
- [add predefined procedures](#) from the Resource Library
- [create new procedures](#) in Procedures Library
- [configure commands for procedures](#) in Procedures Library
- [use the Flow Editor](#) and other configurations required
- [creating a procedure from scratch](#)

## Add Predefined Procedure

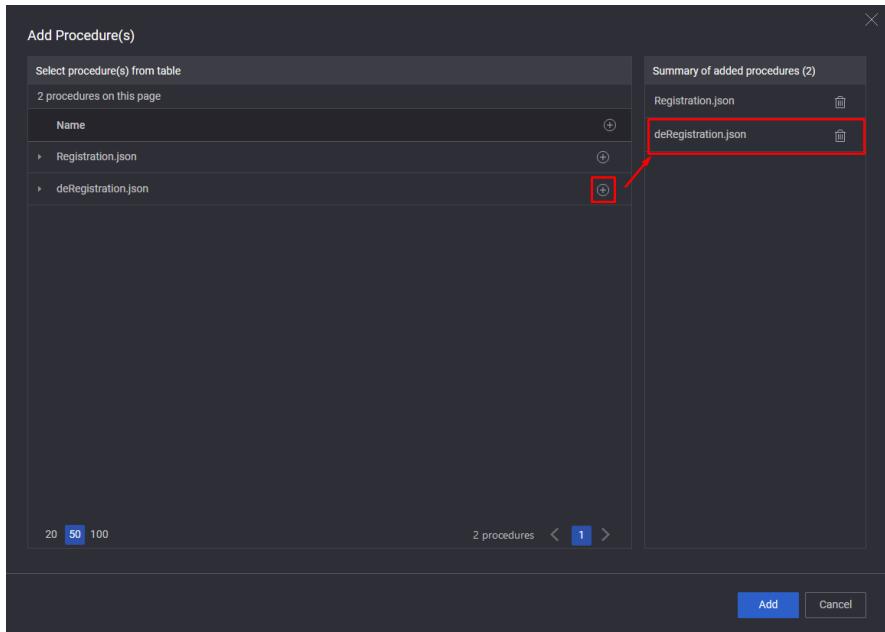
Predefined procedures will be either available upon LoadCore installation, or delivered separately and [imported in the Resource Library](#).

To add procedures from the Resource Library to the Procedures Library:

1. Go to the **Test Overview page > Procedures Library**, or access the **Flow Editor** (see [Voice](#) application traffic).
2. Select one of the categories available (SIP, Media or Flow).
3. To add a predefined/existing procedure, press the **Add Predefined**  button.



4. In the dialog window, select one or more procedures from the existing list by pressing the  icon.



5. To complete the step, click **Add**.

The following step is to configure the procedures.

### Create new procedures

To create new procedures directly in to the Procedures Library:

1. Go to the **Test Overview page** and search for the **Procedures Library** (or access **UE > Range > User Plane > Voice** application traffic > set **Call Type** as *Custom Flow*, then access the **Flow Editor > Procedures Library**).
2. Select one of the categories available (SIP, Media or Flow).
3. Press the **Create New** button ().
4. Configure the new procedure by completing its content, defined in the following fields:

<b>Setting</b>	<b>Definition</b>
Type	Select the type of procedure that will be later This type is later used in the Flow Editor indentation. Note that each category has its own types:

<b>Setting</b>	<b>Definition</b>		
	<b>Category</b>	<b>Type Name</b>	<b>Definition</b>
	<b>SIP</b>	Registration	This type should be selected for procedures in which UE registers to the IMS. For example, <i>Registration Subscribe waitNotify</i> procedures located in the predefined procedures.
	Deregistration		This type should be selected for procedures in which UE deregisters from the IMS. For example, <i>deReg-UnSub-waitNotify</i> procedures located in the predefined procedures.
	Initiate Call		This type should be used for procedures in which the UE is configured to start an SIP call, or wait for one. For example, for <i>MO call setup, MT call setup, MO IMS call setup, MT IMS call setup</i> procedures located in the predefined procedures.
	End Call		This type should be used for procedures in which the UE is configured to end a SIP call, or expect to endone. For example, <i>MO end call, MT end call</i> procedures located in the predefined procedures.
	<b>Media</b>	MEDIA Session	This type should be used for procedures that includes functions that generates media traffic, such as <i>RTP Talk</i> procedure from the predefined procedures.
	<b>Flow</b>	Start	This type should be used for the <i>Start</i> procedure. Unlike the above procedures that includes functions which generate/wait a SIP message or media traffic, this procedure contains only the <i>Start</i> function that marks the start of an iteration.

Setting	Definition		
	Category	Type Name	Definition
		<b>Think</b>	This type should be used for the <i>Start</i> procedure. Unlike the above procedures that includes functions which generate/wait a SIP message or media traffic, this procedure contains only the <i>Think</i> function.
		Stop	This type should be used for the <i>Start</i> procedure. Unlike the above procedures that includes functions which generate/wait a SIP message or media traffic, this procedure contains only the <i>Start</i> function that marks the end of an iteration.
<p><b>NOTE</b> Only the <b>Flow &gt; Start</b> and <b>Flow &gt; Stop</b> procedures are composed from only one command (<i>Flow_Start</i> and <i>Flow_Stop</i>). For the other types, the presence of both <i>Flow_Start</i> and <i>Flow_Stop</i> is mandatory.</p>			
Name	Add the name of the procedure. When the procedure Type is configured, the name is modified to a default value depending on the chosen type. If another name is desired, click in the field and modify the name.  <b>NOTE</b> If the name is similar to another procedure in the list, it will append a number at the end of the name.		
	Click to delete the procedure from the list.		
	Press to drag the procedure up or down and change the order of the procedures.		
Procedures Settings:	<i>Select the procedure to open the content configurator.</i>		
	Select to delete the procedure		
Import or Select Procedure	Select this field if you want to import or reuse the configuration of another procedure. You can: <ul style="list-style-type: none"> <li>• select an existing procedure from the drop-down list</li> <li>• use <b>Upload</b> to import a new procedure into the system; the new procedure will be automatically added to the Resource Library</li> </ul>		

Setting	Definition
	Use <b>Clear</b> to remove any configuration and start and add Commands from scratch.
Save Changes As a New Procedure	This button becomes active if you make changes in the procedure: add/delete commands, or modify the component of a command. Use this button to save the modified procedure with a new name.
<i>Commands:</i>	<i>This section will list all the commands available for a procedure (either imported, or newly added commands).</i>
	Select the <b>Create New</b> button to add new commands to the current procedure.
	This button becomes available only if the list is already populated. Once pressed, it will allow you to search and select commands, to further delete them (either in bulk, or individually).

5. For any command added to the list, use the  con to move the command up or down and redo the order of the commands, or  to remove the command from the list.

Next step is to configure each command in the list.

## Configure commands

Any command in the list, existent or new, can be configured. Click on a command to open the Command panel. The following options are available:

Setting	Definition
	Select the <b>Delete Command</b> button to remove a command from the list.
Type	Select the type of the command. Available options are: <ul style="list-style-type: none"> <li>• <a href="#">SIP_Send_Request</a></li> <li>• <a href="#">SIP_Wait_Response</a></li> <li>• <a href="#">SIP_Send_Response</a></li> <li>• <a href="#">SIP_Wait_Request</a></li> <li>• <a href="#">RTP_Listen</a></li> <li>• <a href="#">RTP_Talk</a></li> <li>• <a href="#">RTP_Control</a></li> <li>• <a href="#">Flow_Start</a></li> <li>• <a href="#">Flow_Think</a></li> <li>• <a href="#">Flow_Stop</a></li> </ul>

### SIP\_Send\_Request command settings

<b>Setting</b>	<b>Definition</b>
Name	The name of the current command. You can leave the default value, or add your own.
Delay Before Execution (ms)	Set the amount of time to delay this procedure from execution.
Success Next Command	<p>Select the next command the UE will be connected to if the command is successful. Here is an example of options available:</p> <ul style="list-style-type: none"> <li>• <i>Start</i></li> <li>• *Send <i>REGISTER</i></li> <li>• *Wait 401 200 <i>REGISTRATION</i></li> <li>• *Send <i>Auth REGISTER</i></li> <li>• *Wait 200 <i>REGISTRATION</i></li> <li>• *Send <i>SUBSCRIBE</i></li> <li>• *Wait 200 <i>SUBSCRIBE</i></li> <li>• *Wait <i> NOTIFY</i></li> <li>• *Send 200 <i> NOTIFY</i></li> <li>• <i>Stop</i></li> <li>• *Send <i>Request</i></li> </ul> <p><b>IMPORTANT</b> The names with an asterisk are depicted from a procedure flow list. The names that will appear for selection depend on the names you are giving to the commands in the Commands list.</p>
Error Next Command	Select the next command the UE will be connected to if the command is not successful.
Method	<p>Select the SIP Method used to construct the SIP Request. The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>INVITE</i></li> <li>• <i>ACK</i></li> <li>• <i>BYE</i></li> <li>• <i>CANCEL</i></li> <li>• <i>OPTIONS</i></li> <li>• <i>REGISTER</i></li> <li>• <i> NOTIFY</i></li> <li>• <i>SUBSCRIBE</i></li> <li>• <i>REFER</i></li> <li>• <i>MESSAGE</i></li> <li>• <i>PRACK</i></li> </ul>

<b>Setting</b>	<b>Definition</b>
	<ul style="list-style-type: none"> <li>• <i>INFO</i></li> <li>• <i>UPDATE</i></li> </ul>
Message Content	<p>The message content that will be displayed when selecting Method. In this section, the message headers are defined. Headers can be automatically constructed based on the settings from the <b>Voice</b> objective or <b>Custom Headers</b>.</p>
Message Body	<p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>None</i></li> <li>• <i>Automatic</i></li> <li>• <i>Custom</i></li> </ul> <p>Depending on the selection, the constructed SIP request can have no body, an automatically constructed body based on the settings from <b>Voice</b> objective, or a Custom body. If <i>Custom</i> is selected, there are templates available from where you can start constructing (see Body Template parameter).</p>
Body Template	<p><b>IMPORTANT</b> This parameter becomes available only if <b>Message Body</b> is set as <b>Custom</b>.</p> <p>Select from the drop-down list the type of template to be used for this message body.</p>
Body	<p><b>IMPORTANT</b> This parameter becomes available only if <b>Message Body</b> is set as <b>Custom</b>.</p> <p>Based on the selected Body Template option, this field will be populated accordingly. You can then modify the value for your procedure needs.</p>
Dialog Action Type	<p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>None</i></li> <li>• <i>New</i></li> <li>• <i>Existing</i></li> </ul> <p>Depending on the selected SIP Method and the desired SIP flow, the <b>Call ID</b> header will be constructed.</p> <p>For example, a Register request can be configured as <i>None</i> <b>Dialog Action Type</b>, for Invite request, <i>New</i>, and for sending an Invite or Update request sent inside the SIP dialog, <i>Existing</i>.</p>
Call ID	<p><b>IMPORTANT</b> This parameter becomes available only if <b>Dialog Action Type</b> is set as <b>Existing</b>.</p> <p>Select from the list the Call ID.</p>

Setting	Definition
Description	Add a description of the configured procedure.
Extract List	Use the <b>Create New</b> button to add a list of predefined SIP Headers, and store the value to a list of predefined variables. These variables can be later used in the construction of subsequent SIP requests/SIP responses.

### SIP\_Wait\_Response/Request command settings

Setting	Definition
Name	The name of the current command. You can leave the default value, or add your own.
Delay Before Execution (ms)	Set the amount of time to delay this procedure from execution.
Timeout (ms)	Set the timeout amount for receiving the message/request. If no message/request is matched from the Status Code list in the configured time, the command will exit on <b>Timeout Next Command</b> output.
Timeout Next Command	Select the next command the UE will be connected to if the command reports a timeout error.  <div style="border: 1px solid #ccc; padding: 5px; margin-left: 20px;"> <b>IMPORTANT</b> The names that will appear for selection depend on the names you are giving to the commands in the Commands list.     </div>
Error Next Command	Select the next command the UE will be connected to if the command is not successful.
Description	Add a description of the configured procedure.
Templates	This section provides a <b>Status Code</b> (for <b>SIP_Wait_Response</b> only), where the user needs to configure the status code of the expected messages/requests, and then select an output (from the configured commands) that the UE will exit if the response is matched.  The best practice is to first configure the commands, and then configure the outputs. There can be multiple expected messages/requests, but each message/request needs to have a separate entry. Optionally, for each entry, user has the option to also extract information and store it in one of the available variables (see <b>Extract List</b> ).
Extract List	For <b>SIP_Wait_Request</b> procedure, use the <b>Create New</b> button to add a list of predefined SIP Headers, and store the value to a list of predefined variables. These variables can be later used in the construction of subsequent SIP requests/SIP responses.

Setting	Definition
	For <b>SIP_Wait_Response</b> , this is integrated under <b>Templates &gt; Status Code</b> line.

### SIP\_Send\_Response command settings

Setting	Definition
Name	The name of the current command. You can leave the default value, or add your own.
Delay Before Execution (ms)	Set the amount of time to delay this procedure from execution.
Success Next Command	Select the next command the UE will be connected to if the command is successful.  <b>IMPORTANT</b> The names that will appear for selection depend on the names you are giving to the commands in the Commands list.
Error Next Command	Select the next command the UE will be connected to if the command is not successful.
Message Content	The message content that will be displayed when selecting Method. In this section, the message headers are defined. Headers can be automatically constructed based on the settings from the <b>Voice</b> objective or <b>Custom Headers</b> .
Message Body	<p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>None</i></li> <li>• <i>Automatic</i></li> <li>• <i>Custom</i></li> </ul> <p>Depending on the selection, the constructed SIP request can have no body, an automatically constructed body based on the settings from <b>Voice</b> objective, or a Custom body. If <i>Custom</i> is selected, there are templates available from where you can start constructing (see Body Template parameter).</p>
Body Template	<b>IMPORTANT</b> This parameter becomes available only if <b>Message Body</b> is set as <b>Custom</b> .  Select from the drop-down list the type of template to be used for this message body.
Body	<b>IMPORTANT</b> This parameter becomes available only if <b>Message Body</b> is set as <b>Custom</b> .  Based on the selected Body Template option, this field will be populated accordingly. You can then modify the value for your

<b>Setting</b>	<b>Definition</b>
	procedure needs.
Request Answered Type	<p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <i>Last Received</i> - if selected, it means that the message is constructed with the information from the last received SIP request</li> <li>• Containing Via Branch - if selected, it will generate the Via Branch parameter</li> </ul> <p>If "Last received". If "Containing Via Branch",</p>
Via Branch	<p><b>IMPORTANT</b> This parameter becomes available only if <b>Request Answered Type</b> is <i>Containing Via Branch</i>.</p> <p>Select from the list the necessary branch. This option can be used when multiple requests are being sent during IMS call setup, and the message needs to be sent with the <b>Via Branch</b> header from the initial request. Using this configuration implies that the via branch was stored in <code>\$SIP_ViaBranch</code> variable in the initial request.</p>
Description	Add a description of the configured procedure.
Extract List	Use the <b>Create New</b> button to add a list of predefined SIP Headers, and store the value to a list of predefined variables. These variables can be later used in the construction of subsequent SIP requests/SIP responses.

### RTP\_Listen command settings

<b>Setting</b>	<b>Definition</b>
Name	The name of the current command. You can leave the default value, or add your own.
Delay Before Execution (ms)	Set the amount of time to delay this procedure from execution.
Duration (ms)	Set the time (in milliseconds) in which the UE sleeps.
Success Next Command	<p>Select the next command the UE will be connected to if the command is successful.</p> <p><b>IMPORTANT</b> The names that will appear for selection depend on the names you are giving to the commands in the Commands list.</p>
Error Next Command	Select the next command the UE will be connected to if the command is not successful.
Description	Add a description of the configured procedure.

### RTP\_Talk command settings

Setting	Definition
Name	The name of the current command. You can leave the default value, or add your own.
Delay Before Execution (ms)	Set the amount of time to delay this procedure from execution.
Duration (ms)	Set the time (in milliseconds) in which the UE generates media.
Non Blocking	If enabled, it will allow the UE to catch SIP messages during media streaming. See <a href="#">Non-blocking behavior</a> for more information.
Success Next Command	Select the next command the UE will be connected to if the command is successful.  <div style="background-color: #005a7b; color: white; padding: 2px 10px; border-radius: 5px; text-align: center;">IMPORTANT</div> The names that will appear for selection depend on the names you are giving to the commands in the Commands list.
Error Next Command	Select the next command the UE will be connected to if the command is not successful.
Description	Add a description of the configured procedure.

### RTP\_Control command settings

Setting	Definition
Name	The name of the current command. You can leave the default value, or add your own.
Delay Before Execution (ms)	Set the amount of time to delay this procedure from execution.
Duration (ms)	Set the time (in milliseconds) in which the UE generates media.
Action	Select to either <b>Terminate RTP</b> , or <b>Wait for RTP Completion</b> . When configured, it needs to be used in relation with the <b>Non blocking</b> option from RTP_Talk command. See <a href="#">Non-blocking behavior</a> for more information.
Success Next Command	Select the next command the UE will be connected to if the command is successful.  <div style="background-color: #005a7b; color: white; padding: 2px 10px; border-radius: 5px; text-align: center;">IMPORTANT</div> The names that will appear for selection depend on the names you are giving to the commands in the Commands list.
Error Next Command	Select the next command the UE will be connected to if the command is not successful.

Setting	Definition
Description	Add a description of the configured procedure.

### Flow\_Start/Flow\_Think/Flow\_Stop command settings

Setting	Definition
Name	<p><b>IMPORTANT</b> This parameter appear only for <i>Flow_Start</i> or <i>Flow_Think</i> commands.</p> <p>The name of the current command. You can leave the default value, or add your own.</p>
Duration (ms)	<p><b>IMPORTANT</b> This parameter appear only for <i>Flow_Think</i> commands.</p> <p>Set the time (in milliseconds) in which the UE sleeps.</p>
Success Next Command	<p>Select the next command the UE will be connected to if the command is successful.</p> <p><b>IMPORTANT</b> The names that will appear for selection depend on the names you are giving to the commands in the Commands list.</p>
Description	Add a description of the configured procedure.

## Flow Editor

After procedures become available in the Procedures Library, you can construct the state machine in the Flow Editor to obtain the desired SIP flow. The flow configuration steps are as follows:

1. In a test, create two UE ranges.
2. On each UE range, go to **Objectives > User Plane > Application Traffic > Voice** and set the **Call Type** as **Custom Flow**.

The **Flow Editor** becomes available.

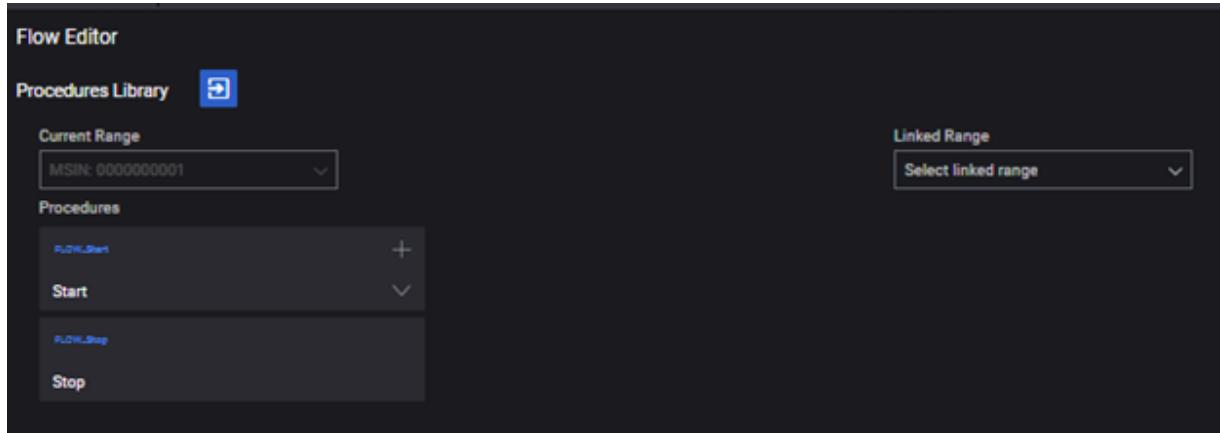
3. Press  to open the editor's window and start configuring the flow.

**IMPORTANT** When you open the Flow Editor on a new test, you will have to first add the *Stop* and the *Start* procedures. If no procedure is available, this means that *Start* and *Stop* procedures do not have a *Type* configured in the Procedures Library. See [Procedures Library](#) for adding predefined procedures or creating new.

**NOTE** For details on the configuration parameters found under Procedures Library, see **Voice** objective.

4. In the **Flow Editor** page, configure the procedures under the **Current Range** (automatically selected).

5. First, add the *Stop* and the *Start* procedures. In the **Add required procedures first**, click on the *Select FLOW\_Stop\_procedure* field to see the options, and choose the *Stop* procedure that has been previously added in the **Procedures Library > Flow** section.
6. Similarly, click on the *Select FLOW\_Start\_procedure* field to see the options, and choose the *Start*.



7. You can now configure the state machine for both MO and MT side: on the **Linked Range** option on the right side, select the UE range created and configured at **Steps 1 and 2**. Then, repeat **Steps 5 and 6** on the linked range. Now both procedures are linked and have the same start and stop procedures added.



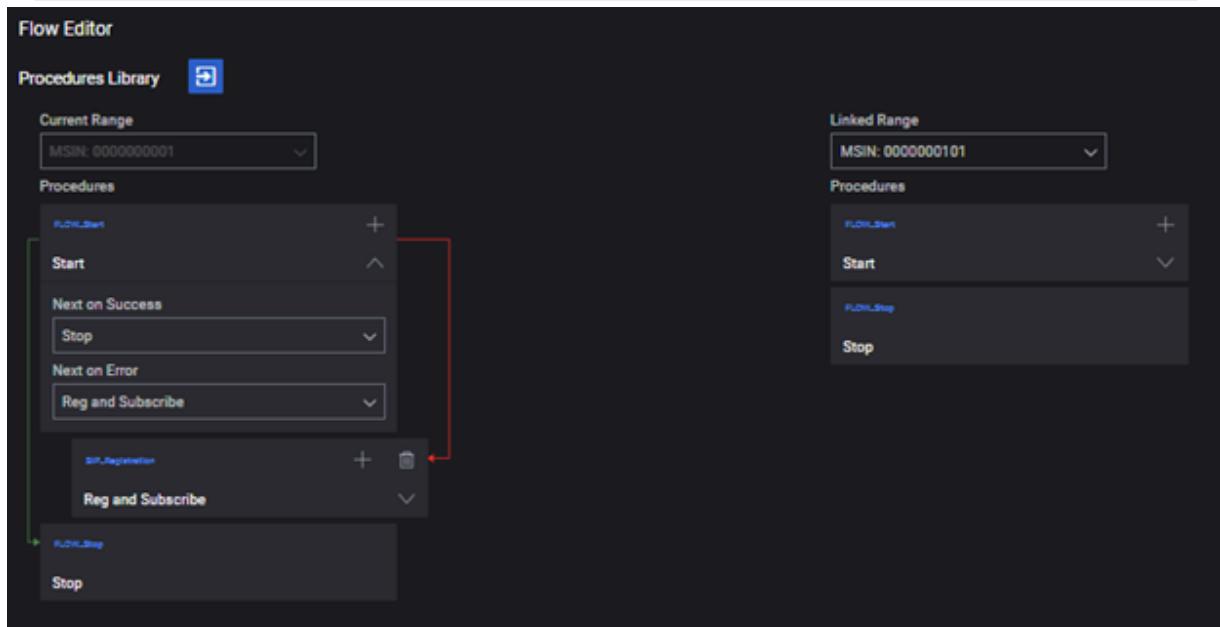
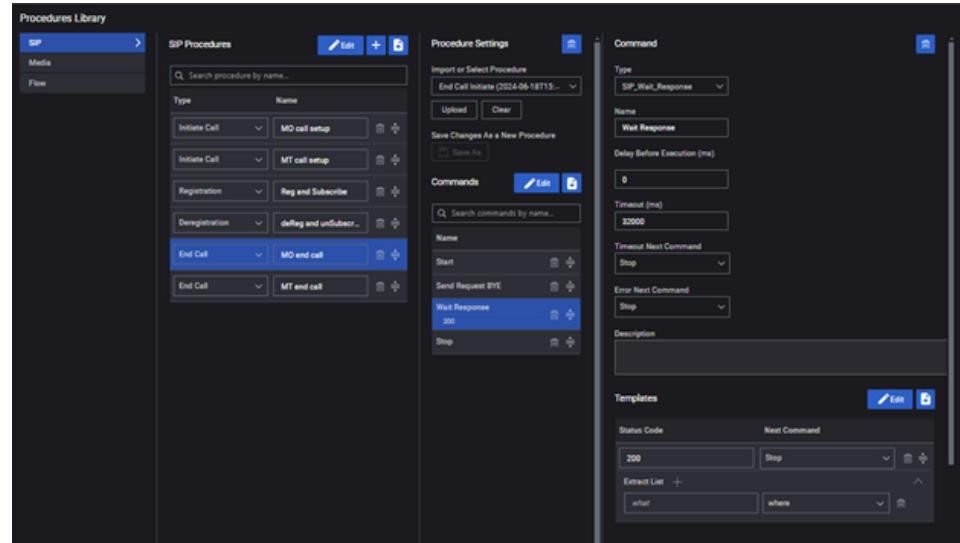
8. Use the **+**button from the *Start* tile, then **Add Procedure** to add more procedures in between the two. A drop-down list appears, including all the procedures available.
9. Select the *Reg and Subscribe* procedure. Note that each procedure added (except the *Stop* block) has an expand button, and includes two configuration selections:
  - **Next on Success** - select from the drop-down which procedure will follow if the current one is successful, or leave the default (*None*);
  - **Next on Error** - select from the drop-down which procedure will follow if the current one fails, or leave the default (*None*).

**NOTE**

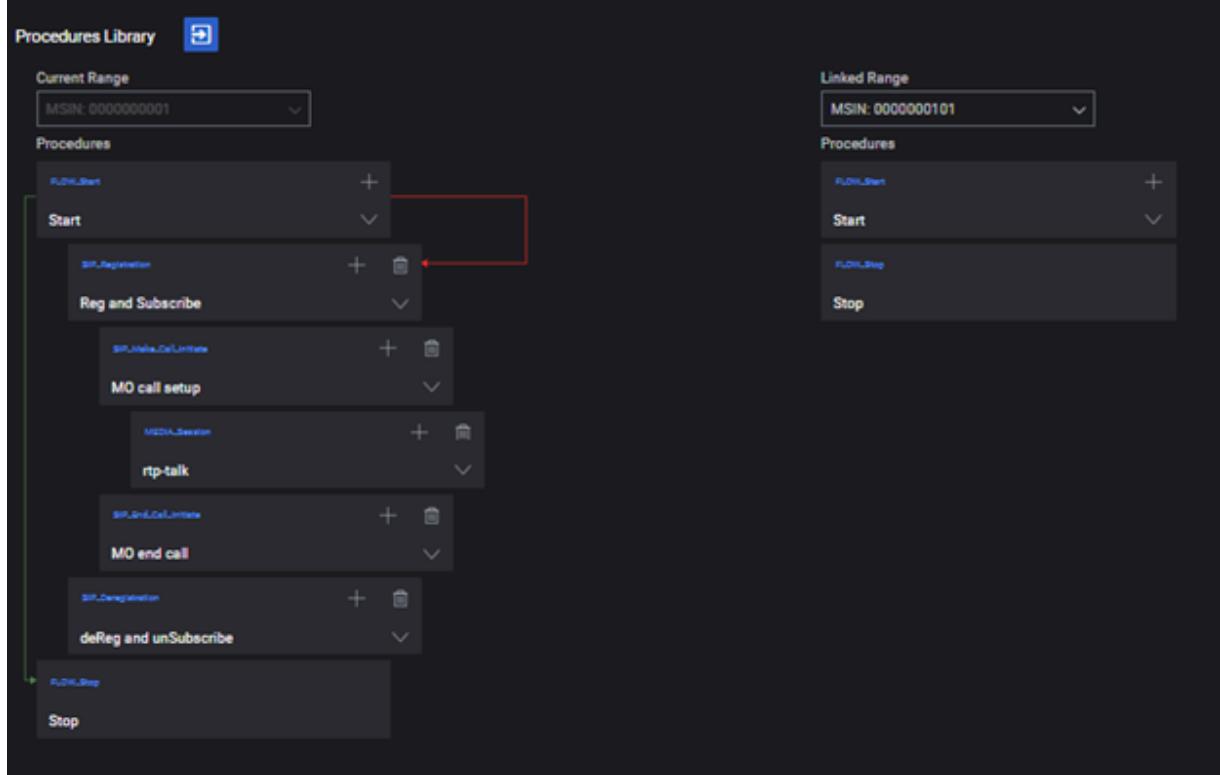
Each procedure needs to be connected, by adding an option to these fields. For easy reading of the configuration, the blocks are connected via blue arrow lines on the left, showing the procedures that follow when successful, and red arrow lines on the right, indicating which connection follows when in error.

**IMPORTANT**

The mechanism based on which the UE will exit on a certain output depends on the output that UE will exit on the commands defined inside the procedure.

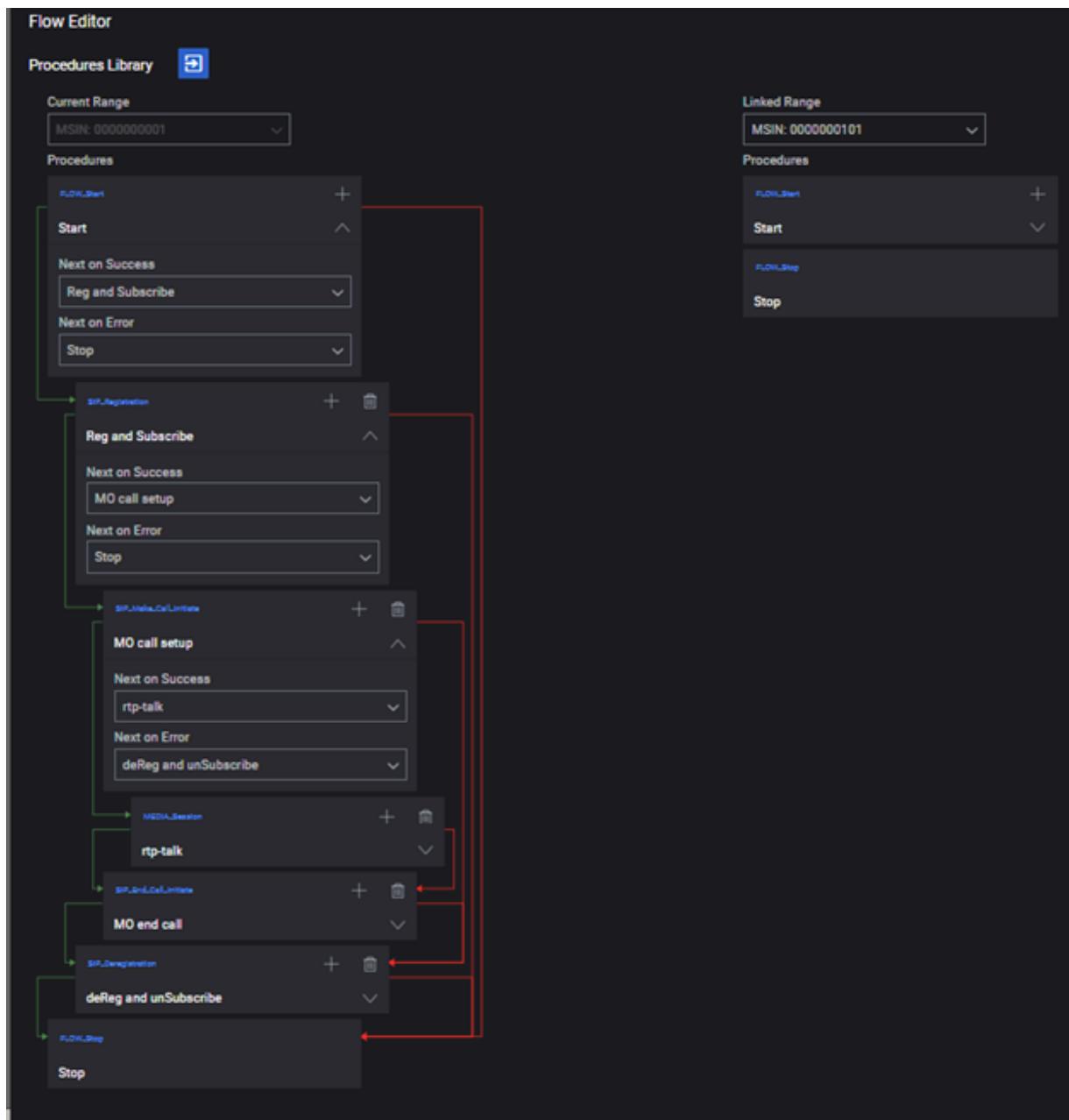


- Add the rest of the procedures, for example: *Mo call setup, Rtp-talk, Mo end call, deReg and Unsubscribe*. Remember they have to be previously configured in the Procedures Library.

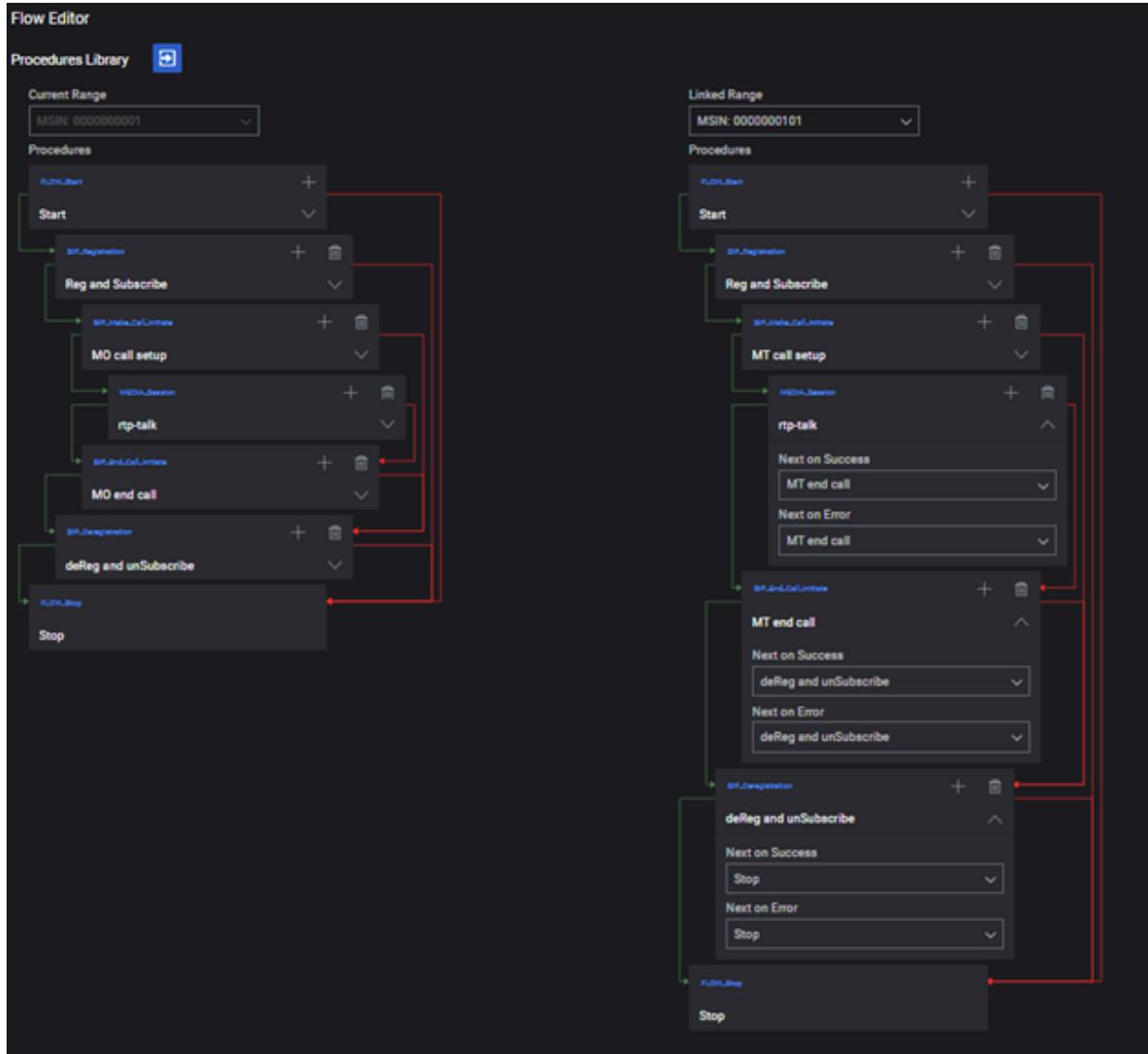


11. Note that there are three outputs defined on a command in the Procedure Library: *Timeout Next Command*, *Error Next Command* and *Next Command*:
- when UE will exit on a *Timeout Next Command* (which means the expected message was not received on the configured timeout value) or *Error Next Command*, it means the UE will exit on the **Next on Error** output from the procedure added in the Flow Editor.
  - when UE will exit on the *Next Command* exit, it means the UE will exit on the **Next on Success** procedure's output displayed in Flow Editor.

You need to connect the outputs as shown in the following image:



12. In a similar manner, proceed to configure the state machine on the MT side, from the **Linked Range** section.



## Debugging

If, for some reason, the user forgets to connect any output, either from inside the procedure or the main procedure, the following error will be thrown, indicating the UE range, procedure name and command name:

```
"Test stopped: 10.38.157.137 - Error on ng-ran node: HTTP PUT request failed on URL:  
http://localhost:80/api/v1/applications/ng-ran/configuration with error: For UE range with SIP  
phone 10000000100, for procedure MO call setup, the 'Next on Success' output is not connected.
```

This type of error message can also appear if the outputs are not connected.

To debug the SIP call flow (recommended for functional testing):

1. Go to **Overview > Global Settings > Advanced Settings**
2. On the **Log level** parameter, select **Debug**.
3. On the **Log Tags** parameter, select **Media**.

In these files, you log each input and output that the UE entered/exited in/from procedures, as well as the SIP messages sent and received.

4. After running the test, connect via SSH to the agent on which RAN is mapped, and go to `/opt/5gc-test-engine/logs`. When using the above debug combo, a debug file will be created per UE.

**IMPORTANT**

Performance testing is not recommended when debugging is enabled.

## UE Range Configuration

After the Flow Editor configuration is complete, there are several configurations to consider on each UE range, in the [Voice](#) configuration panel (refer to the respective section for complete description of the parameters):

Section	Parameter(s)	Configuration description
<b>Dial Plan</b>	Source Phone <b>Destination Phone</b>	The IMISDN is configurable in the Range Settings, Identification section and in Dial Plan is visible only for visualization.
	Destination IP	Should be the real or the simulated IMS IP.
	Iterations	Set the amount of time that the state machine configured in Flow Editor will be repeated ( <b>0</b> meaning infinite loops).
<b>SIP Settings</b>	Transport Protocol	Select either <b>TCP</b> or <b>UDP</b> .
	Domain	Select the IMS domain.
	Enable IPSec	If enabled, the current behavior is that the UE will negotiate and initiate an IPSec tunnel towards IMS.
	Registration Refresh Time	There are two available options that can be selected: <ul style="list-style-type: none"> <li>• <b>Negotiated</b>- means the UE will send a register refresh at 50% out of the expires value advertised by IMS.</li> <li>• <b>Custom</b>- means thata the UE will send a register refresh after the custom value configured by the user.</li> </ul>
	Number of Loops after the Registration to Send Deregistration	This configures the number of loops performed by UE after a successful registration, when the UE will first deregister, then register again to the IMS. Value meaning: <ul style="list-style-type: none"> <li>• <b>0</b> implies that UE deregistration is performed at the end of the last loop.</li> <li>• <b>1</b> means that UE deregistration and</li> </ul>

<b>Section</b>	<b>Parameter(s)</b>	<b>Configuration description</b>
		<p>registration will be done during every loop.</p> <ul style="list-style-type: none"> <li>• <b>n</b> (where <math>n &gt; 1</math>) means that UE deregistration and registration will be done every <b><i>n<sup>th</sup></i></b> loop.</li> </ul>
<b>SIP Settings &gt; Advanced SIP Settings</b>		
SIP Authentication	Username	The username from the Authentication header from Register request is constructed automatically based on IMSI and domain name.
	K OP or OPc	Configure all these parameters.
Custom Parameters		<p>The only configurable item from this section is <i>MaxActiveLimit</i>. It is recommended not modifying this value, unless instructed to do so.</p> <p>The rest of the items are applicable when using call type: basic call, basic call MO and basic call MT.</p>
SIP 3GPP IPsec	Port-C Port-S Authentication Algorithm Encryption Algorithm	All these parameters can be modified.
	Use same connection for Registration and Calls	If enabled on the UE range on which you expect to receive the call setup, then <i>Register</i> and <i>Invite</i> requests will be received on the same connection.
<b>RTP Settings</b>	Local Port	Can modify (if needed).
	RTP Session Duration	Note that this parameter does not modify the duration of the RTP Talk procedure; when using custom flow, the Talk Time is configurable directly on the <i>RTP_Talk</i> command.

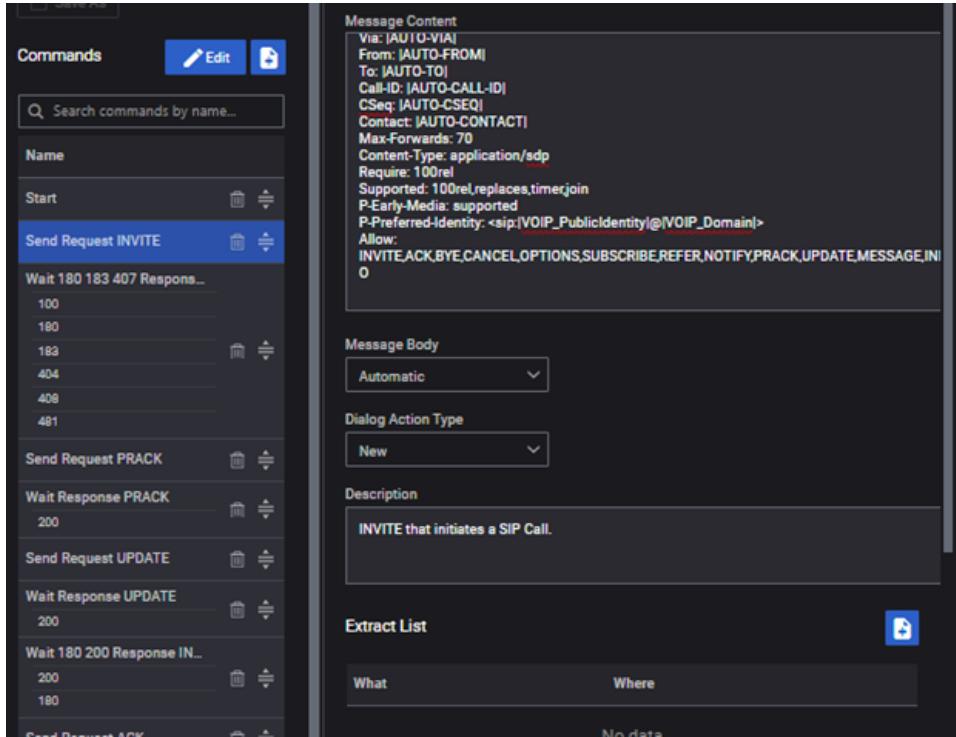
Section	Parameter(s)	Configuration description
<b>Audio Settings</b>	Enable Audio	The audio traffic can be enabled/disabled.
	QoS Flow ID for Voice	Allows audio RTP mapping, if the QoS flow has been configured in <b>Global Settings &gt; QoS Flow</b> .
	Audio Codecs	You can select the audio codecs required for the test-case.
	*SDP Body configuration	<p>The SDP body is configurable from inside the SIP Procedure: <b>Procedures Library &gt; &lt;Procedure Name&gt;</b>, then select either <i>SIP_Send_Request</i> or <i>SIP_Send_response</i> function and find the <b>Message Body</b> section.</p> <p>SDP construction includes two options:</p> <ul style="list-style-type: none"> <li>• <i>Automatic</i>- the SDP will be constructed based on the codecs available in the RTP Settings; if no codec is defined here, a default codec is used.</li> <li>• <i>Custom Message Body</i> - you can start from a template and modify it accordingly.</li> </ul> <p>To create a signaling-only scenario, disable the Audio Settings (see the above parameter), and the RTP (from <b>Global Settings &gt; Advanced Settings &gt; Traffic Settings, switch off the Enable RTP parameter</b>). In addition, you need to choose a Custom Message Body for SDP body.</p>
<b>Video Settings</b>	Enable Video	The video traffic can be enabled/disabled.
	QoS Flow ID for Video	Allows audio RTP mapping, if the QoS flow has been configured in <b>Global Settings &gt; QoS Flow</b> .
	Video Codecs	You can select the video codecs required for the test-case.
	*SDP Body configuration	Follow the same principles as with the <b>Audio Settings</b> .
<b>MSRP and MCPTT Settings</b> are not validated in the current release, when using a custom flow call type.		

## Dialog Handling

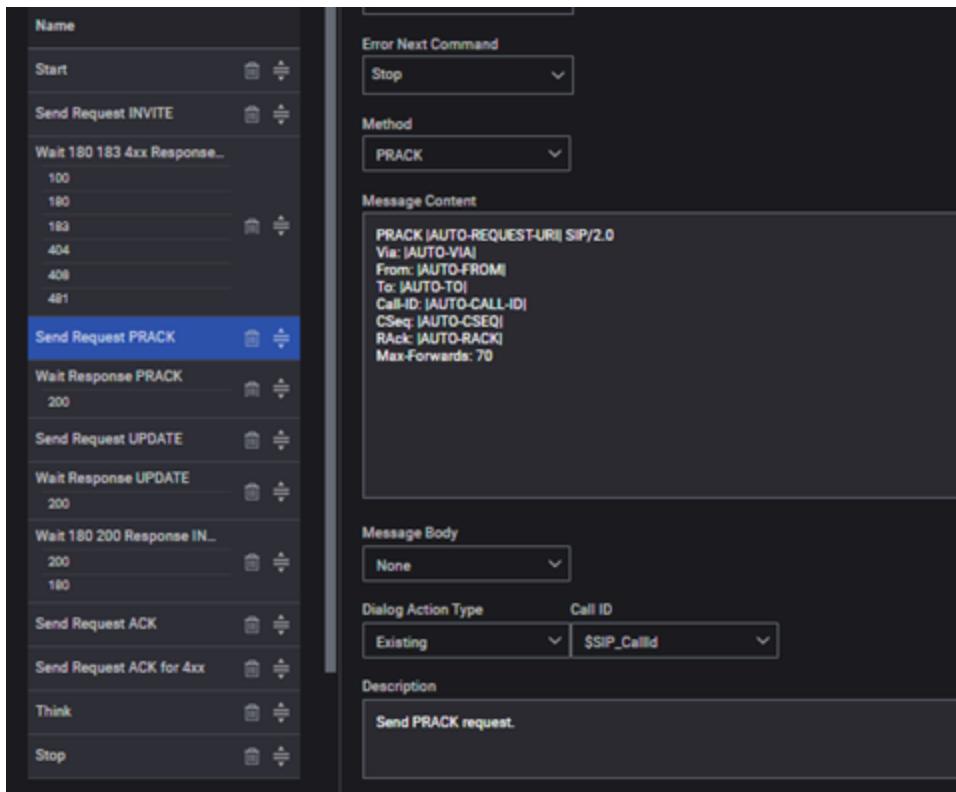
An important aspect regarding SIP Procedures is how the dialog is handled.

On the *SIP\_Send\_Request* functions, the dialog handling is done by configuring the **Dialog Action Type** (and choose between *None*, *New* or *Existing*).

For example, when sending an initial *Invite* request, this request will create a dialog (per RFC 3261 specifications), therefore the **Dialog Action Type** is *New*.



On *Wait\_SIP\_Response*, for each wait message entry, you can extract Call ID in the *\$SIP\_CallID* variable, and configure when to send the next request. Then, when sending the next request, on the same dialog, set the **Dialog Action Type** as *Existing*, and choose the *\$SIP\_CallID* from the Call ID drop-down.



The same principle applies to the MT side: on the *Wait Invite*, extract **Via Branch** in the `$SIP_ViaBranch`, and then use the **Containing Via Branch** in the *Send 180 Ringing* and *200 Ok* messages.

**Top Screenshot: Wait INVITE Command Configuration**

- Type:** SIP\_Wait\_Request
- Name:** Wait INVITE
- Delay Before Execution (ms):** 0
- Timeout (ms):** 3200000
- Timeout Next Command:** Stop
- Error Next Command:** Stop
- Description:** Wait INVITE Request.
- Templates:**
  - Method:** INVITE
  - Next Command:** Send Response 183
  - Extract List:** +  
Via Branch    \$SIP\_ViaBranch

**Bottom Screenshot: Send Response 180 Configuration**

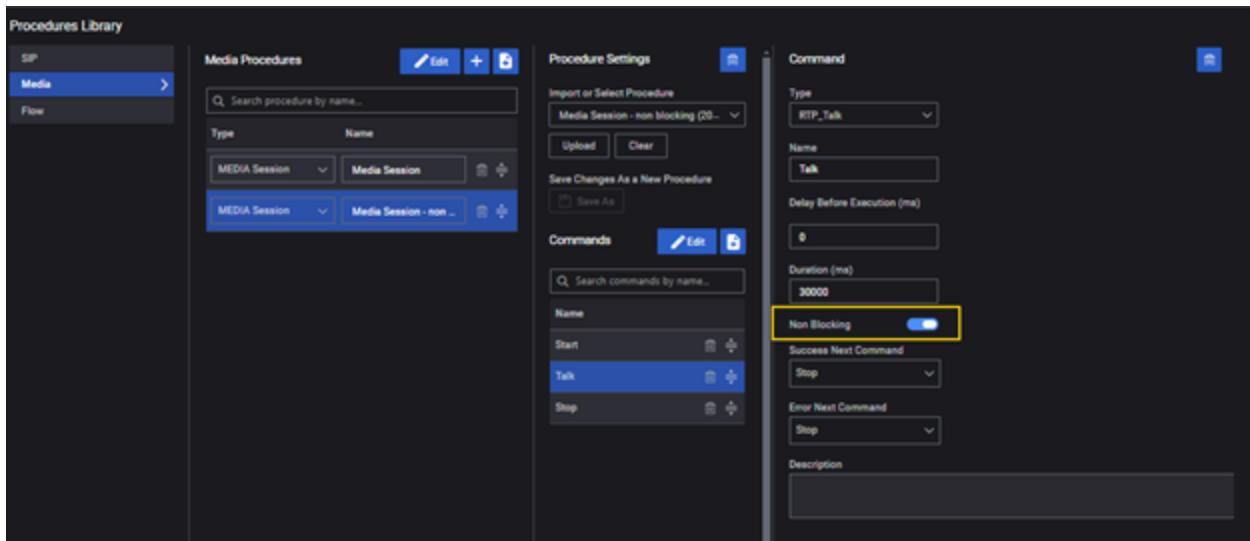
- Type:** SIP\_Send\_Response
- Name:** Send Response 180
- Delay Before Execution (ms):** 0
- Success Next Command:** Send Response 200 INVIT...
- Error Next Command:** Stop
- Message Content:**

```
SIP/2.0 180 Ringing
Via: [AUTO-VIA]
From: [AUTO-FROM]
To: [AUTO-TO]
Call-ID: [AUTO-CALL-ID]
CSeq: [AUTO-CSEQ]
Contact: [AUTO-CONTACT]
Max-Forwards: 69
```
- Message Body:** None
- Request Answered Type:** Via Branch
- Containing Via Branch:** \$SIP\_ViaBranch
- Description:** Sending 180 Ringing to INVITE request.

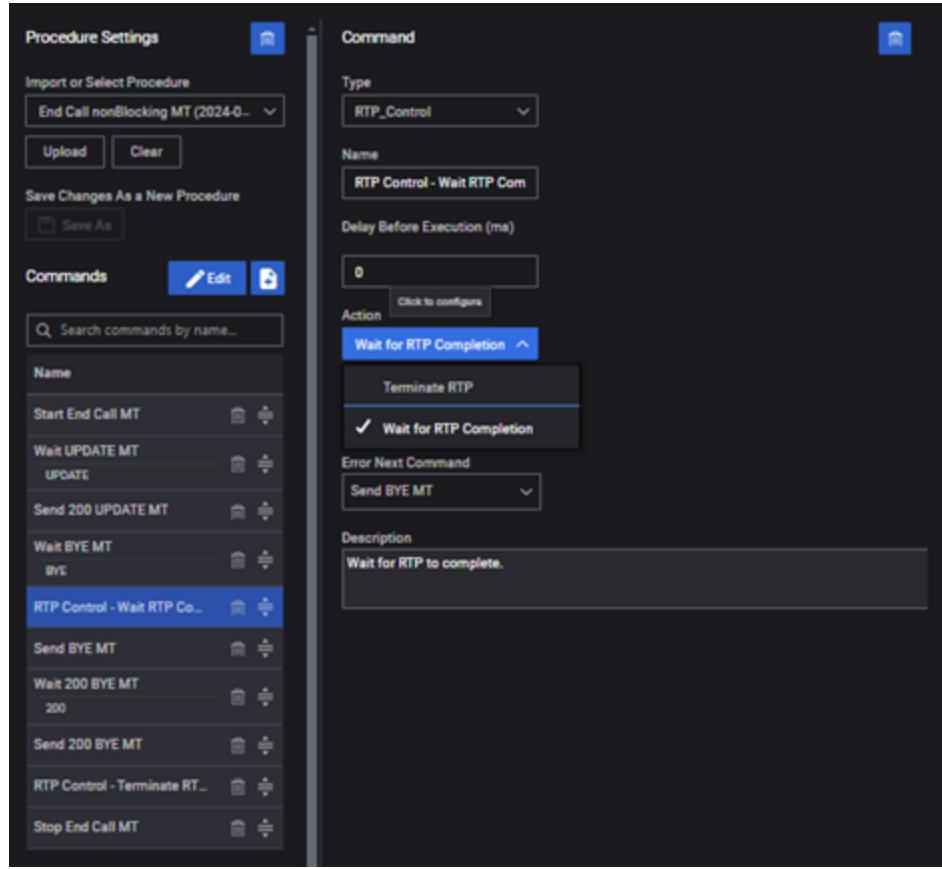
## Non-blocking behavior

There are two behaviors observed on the *RTP\_Talk* command, depending on the **Non-Blocking** option configuration:

- if **disabled** (default)- while UE generates RTP traffic, it remains in the *RTP\_Talk* command, and the commands or commands procedures that follow in the call flow will be executed by the UE after exiting the *RTP Talk* function.
- if **enabled** - while UE generates RTP traffic, the UE exits the *RTP\_Talk* command and continues to execute the commands configured in the call flow. The purpose of this behavior is for the UE to:
  - send *send/wait requests/responses* while sending/receiving RTP traffic.
  - perform different actions, based on the message received. For example, if the UE receives an *Update* request, it will answer and continue the RTP traffic, but if receives a *BYE* request (meaning the call is ended earlier by the corresponding UE or IMS), the UE will respond to the end call request, and stop generating RTP traffic.



When adding the *RTP\_Talk* command with *non-blocking* enabled in the call flow, the *End call* procedure will have the following structure (see image), depending if the UE is an originator (MO) or a terminator (MT). When using the non-blocking functionality, you have to include the *RTP\_Control* function in the flow, which **Action** parameter can be configured to be either *Terminate RTP*, or *Wait for RTP Completion*.



The call flow using non-blocking mechanism includes the following:

- For an MO call setup, set *RTP\_Talk* as Non-Blocking, set *Wait BYE* (with **Timeout** value = RTP duration configured on *RTP\_Talk* command). If:
  - BYE* is received and matched while the UE is in *Wait BYE*, the UE will exit on the **Next Command** output, followed by **RTP Control** with **Action**: *RTP Terminate*, then *Send 200 Ok BYE*.
  - OR
  - BYE* is not received while the UE is in *Wait BYE* command, the UE will exit after the timeout value on the **Timeout Next Command** output, followed by **RTP Control** with **Action**: *Wait for RTP Completion*, then *Send BYE*, and finally *Wait 200 OK BYE*.
- For an MT call setup (MO UE initiates the end call), the order of the events is similar. The difference is that the UE stays more time in the *Wait BYE*. The **Timeout** value = RTP duration configured on *RTP\_Talk* command, plus the default timeout value(32 seconds).

To send a message while the UE generates RTP, you need to insert a *Send Request/Wait Response* before the *Wait BYE* command, and configure the "delay before execution" field (on the Send Request) to specify the amount of time between starting RTP and sending Update request. In this case the call flow will be as shown below:

- On MO side, set the MO call setup flow as *RTP\_Talk* with **Non Blocking** enabled, then *Send UPDATE* (with delay before execution value greater than 0), the *Wait 200 OK UPDATE*, and finally *Wait BYE* (with **Timeout** value = RTP duration configured on *RTP\_Talk* command, minus

the delay before execution). If:

- *BYE* is received and matched while UE is in *Wait BYE* command, the UE will exit on the **Next Command** output, followed by **RTP Control** with **Action**: *RTP Terminate*, then *Send 200 Ok BYE*.  
OR
- *BYE* is not received while UE is in *Wait BYE* command, the UE will exit after the timeout value on the **Timeout Next Command** output, followed by **RTP Control** with **Action**: *Wait for RTP Completion*, then *Send BYE*, and finally *Wait 200 OK BYE*.

- B. On MT side, set the MT call setup flow as *RTP\_Talk* with **Non Blocking** enabled, then, in order, *Wait UPDATE> Wait 200 OK UPDATE > Wait BYE* with the **Timeout** value = RTP duration configured on *RTP\_Talk* command, plus the default timeout value(32 seconds). If:
- *BYE* is received and matched while UE is in *Wait BYE* command, the UE will exit on the **Next Command** output, followed by **RTP Control** with **Action**: *RTP Terminate*, and finally *Send 200 Ok BYE*.
  - OR
  - *BYE* is not received while the UE is in *Wait BYE* command, the UE will exit after the timeout value on the **Timeout Next Command** output, followed by **RTP Control** with **Action**: *Wait for RTP Completion*, then *Send BYE*, and finally *Wait 200 OK BYE*.

## How to create and configure a procedure from scratch

Recommendations on how to configure a procedure:

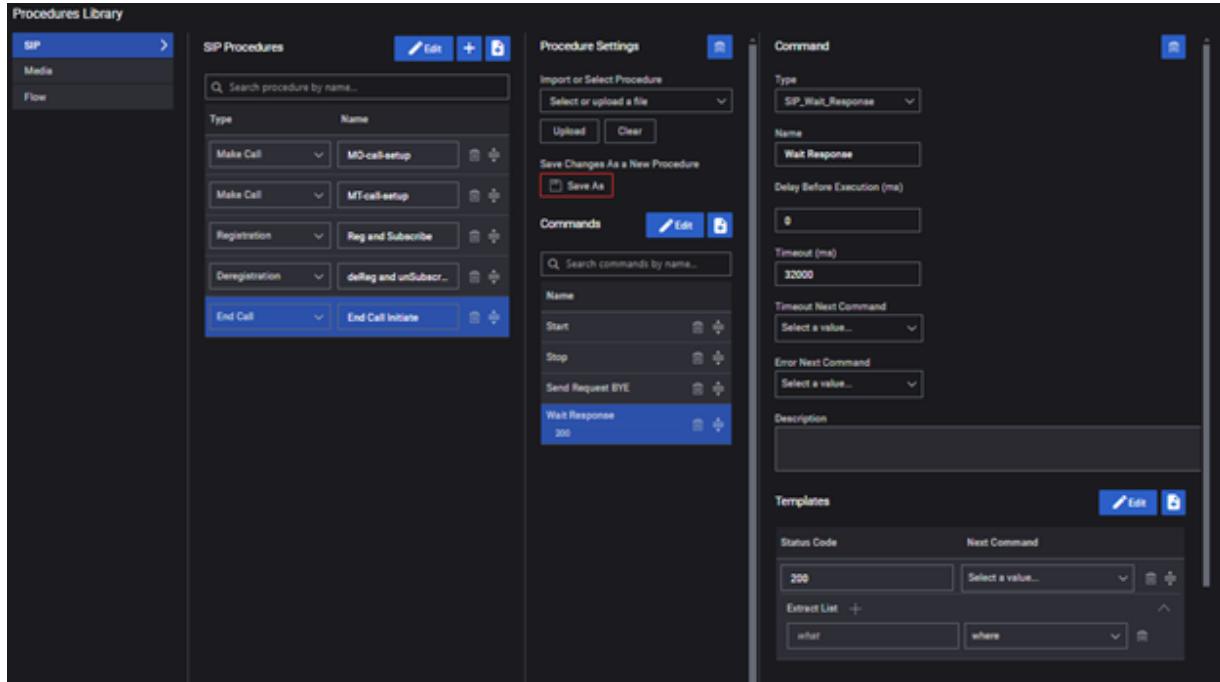
- Add **Start** and **Stop** commands at the beginning and the end of the procedure.
- Between these commands, add the **Wait/Send Requests/Responses** commands .

**IMPORTANT** The order in which the commands are added in the Commands list does not impact the state machine, it is important to connect the output of the commands.

An example of a clean configuration would be:

1. Create an **MO end call** procedure (*Send BYE – Wait 200 OK*) and an **MT end call** procedure (*Wait BYE - Send 200 OK*).
2. For the **MO end call** procedure, from **Procedure Settings > Commands**:
  - add a command and select type *Flow\_Start*.
  - add another command and select type *Flow\_Stop*.
  - add a new command and, in **Command** panel:
    - select Type as *SIP\_Send\_Request*.
    - select Method as *BYE*.
    - select Message body as *None*.
    - select Dialog Action Type as *Existing*, and then set Call ID as *\$SIP\_CallID*. See [Dialog handling](#) for more details.
    - optionally, customize the command Name in the name field.
  - similarly, add a new command:

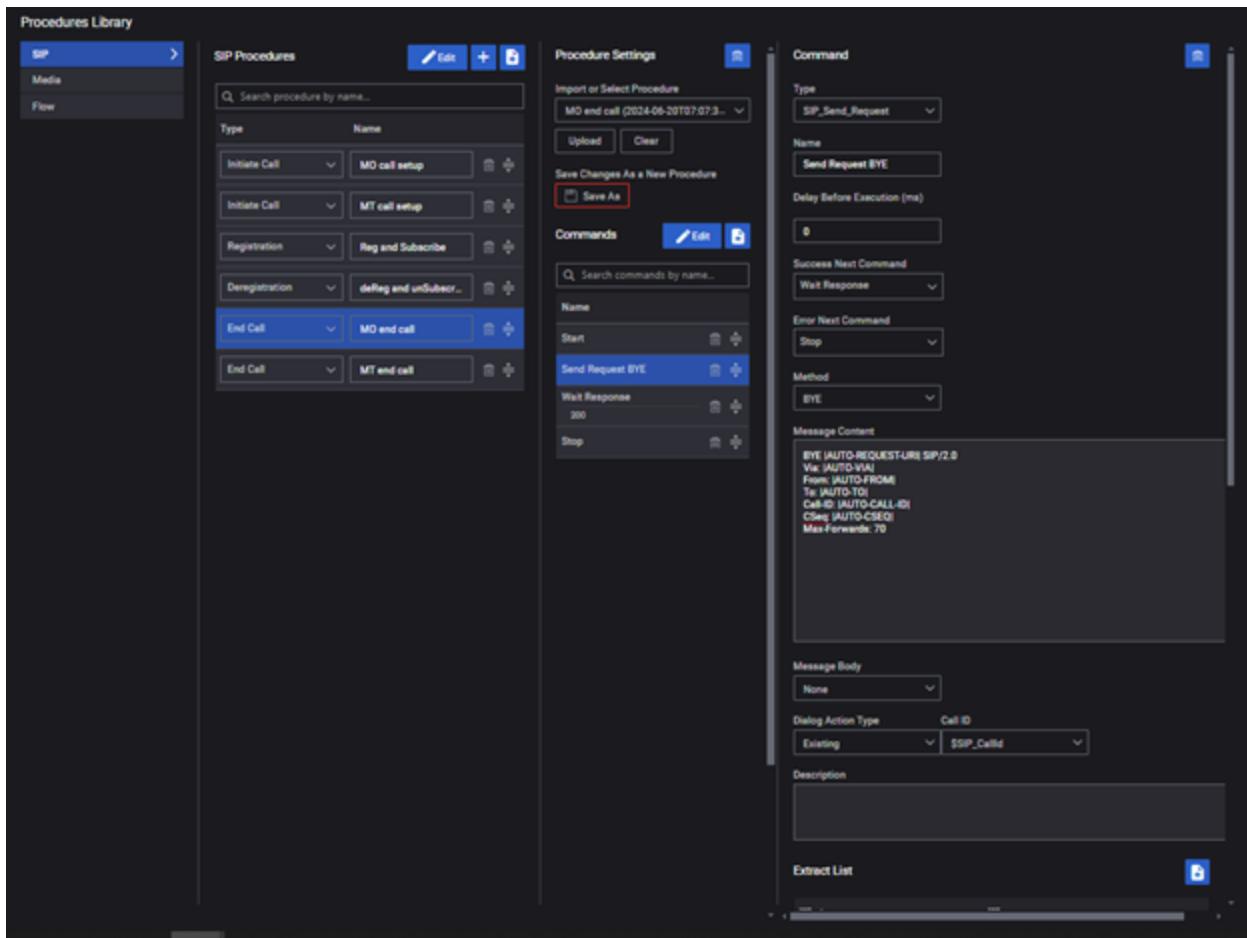
- select the Type as *SIP\_Wait\_Response*.
- configure the Status Code of the message to expect. Under **Templates**, input the value of the status code.
- Optionally, customize the command name in the name field.



At this stage you have all the commands added to the command list. The next step is to connect the output of all the commands. To help visualize the flow you can arrange the commands in the command list, using the click and drag button ( $\triangle$ ) from each command under Procedure Settings.

To connect the output of the commands:

1. On the **Start** command, set the **Success Next Command** to *Send Request BYE*.
2. On the *Send Request BYE*, connect the **Success Next Command** parameter to *Wait Response*, and **Error Next Command** parameter to *Stop*.
3. On the **Wait Response** command, set the:
  - **Next Command** to *Stop*
  - **Timeout Next Command** to *Stop*
  - **Error Next Command** to *Stop*.
4. Save the procedure using the **Save As** button. The procedure will be saved under a JSON file, and will be named with the procedure's name and time stamp.



Use the same steps for the **MT end call** procedure, with the following differences:

- instead of *SIP\_Send\_Request*, configure as *SIP\_Wait\_Request*, and select method *BYE*.
- instead of *SIP\_Send\_Response*, configure as *SIP\_Send\_Response*.
- then, select the outputs on each command:
  - on *Start* command, set **Success Next Command** to *Start*.
  - on *Wait Request BYE*, set **Next Command** to *Send Response BYE*, **Timeout Next Command** and **Error Next Command** to *Stop*.
  - on *Send Response BYE*, set **Success Next Command** to *Stop*, and **Error Next Command** to *Stop*.
- Save the procedure using the **Save As** button.

**IMPORTANT**

If a procedure is modified, the procedure is not saved automatically; the **Save As** button turns red if something is modified in the procedure. Unless the procedure is specifically saved, the previous version will be used in the next test run.

**NOTE**

To save the procedure and another JSON file, you need to first modify an element in the procedure and change the procedure's name. After this, the procedure will be saved under a new JSON with the procedure name and time stamp.

## Custom Fuzzing Scripts

Resource Library holds all uploaded fuzzing scripts listed under the **Custom Fuzzing Scripts**. From **Settings (⚙)** menu > **Library** > **Resource Library** > **Custom Fuzzing Scripts** you can delete, export existing scripts, or import new ones.

**IMPORTANT** This feature manages scripts at global level. At SBI Fuzzer range level, Custom Fuzzing scripts are uploaded and assigned per SBI Fuzzer range (see [SBI Node Settings](#)).

## Export Other Resources

You can export other types of resources besides custom applications from the LoadCore UI, both system resources and custom resources (such as payloads, TLS certificates, TLS keys, TLS DHS, playlists, media files, captures).

To export resources:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library** > **Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select the tab corresponding to the resources you want to export (for example, **Payloads**, **TLS Certificates**, etc.).  
The list of available resources opens.
4. Select the resources you want to export by clicking the check box next to each item, or select all the resources on the page by clicking the check box next to the **Name** column.
5. Click **Export** at the bottom of the resources list. The selected resources are downloaded on your machine as a .zip file. You can use this downloaded archive to import the same resources on other LoadCore setups for example.  
You can also export all the available resources by clicking the **Export all** button under the **Browse resources** pane.

## Import Resources

You can import other types of resources besides custom applications from the LoadCore UI, both system resources and custom resources (such as payloads, TLS certificates, TLS keys, TLS DHS, playlists, media files, captures).

To import resources:

1. Log in to the LoadCore UI.
2. Under the **Settings** menu, select **Library** > **Resource Library**. The Resource Library page opens.
3. Under **Browse resources**, select the tab corresponding to the resources you want to export (for example, **SIP Procedures**, **Payloads**, **TLS Certificates**, etc.).  
The list of available resources opens.
4. Click **Import** at the bottom of the resources list. Select the resources to be loaded from your machine .

**TIP**

When importing a procedure or a configuration that contains procedures, if procedures with the same name and/or content are detected, the application will append a number to their name in order to have unique name for the imported JSON.

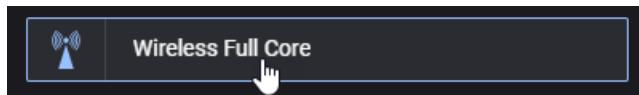
---

This page intentionally left blank.

*CHAPTER 6*

## Full Core tests: configuration settings

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



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

**Topics:**

<b>Global Settings</b> .....	<b>120</b>
Global Settings panel .....	122
Node Start/Stop Rates .....	122
DNS Settings .....	123
Advanced Settings .....	123
DNNs panel .....	127
DNN configuration settings .....	129
Session AMBR configuration settings .....	132
ePCO configuration settings .....	133
Traffic Control Settings configuration .....	134
3GPP RADIUS Server configuration .....	135
Impairment .....	136
QoS Flows panel .....	137
QoS Flow configuration settings .....	138
QoS Flow Packet Filter configuration settings .....	141
QoS Flow Max Packet Loss Rate settings .....	142
QoS Flow ARP configuration settings .....	142
QoS Flow MBR configuration settings .....	143

QoS Flow GBR configuration settings .....	143
CA Certificates .....	143
Milenage .....	144
Customer Parameters .....	145
External Stats Server .....	145
Global Playlists .....	152
<b>UE configuration settings .....</b>	<b>153</b>
UE Ranges panel .....	155
UE Range panel .....	156
Range Settings .....	158
UE Identification settings .....	159
UE Security settings .....	159
UE Settings settings .....	163
UE Shared Data IDs .....	171
UE Subscribed AMBR settings .....	171
Service Area Restriction settings .....	171
Forbidden Areas .....	173
DNNs Config .....	174
Notifications .....	177
SMS Configuration .....	177
Equipment Status .....	180
Converged Charging .....	180
Spending Limit Control .....	181
Internal Group IDs .....	184
Network Slicing settings .....	185
UE NSSAI settings .....	186
UDM Default NSSAI settings .....	187
UDM SNSSAI Mappings .....	187
UDR SNSSAI Settings .....	188
Objectives .....	189
Control Plane Objective .....	190
User Plane Objectives .....	206

<b>3GPP RADIUS Server configuration settings .....</b>	<b>275</b>
3GPP RADIUS Server Ranges panel .....	275
3GPP RADIUS Server Range settings .....	276
3GPP RADIUS Server Node settings .....	277
3GPP RADIUS Server N6 interface settings .....	277
<b>AMF configuration settings .....</b>	<b>280</b>
AMF Ranges panel .....	281
AMF Range settings .....	282
AMF Node settings .....	283
AMF Custom NF Services settings .....	286
AMF N2 interface settings .....	287
AMF Namf interface settings .....	290
AMF N26 Interface Settings .....	292
AMF Remote SBA nodes .....	293
<b>AUSF configuration settings .....</b>	<b>301</b>
AUSF Ranges panel .....	302
AUSF Range panel .....	302
AUSF Node settings .....	303
AUSF Nauf interface settings .....	304
AUSF Remote SBA Nodes .....	307
AUSF Custom NF Services settings .....	309
<b>CHF configuration settings .....</b>	<b>310</b>
CHF Ranges panel .....	310
CHF Range settings .....	311
CHF Node settings .....	312
CHF Nchf interface settings .....	313
CHF remote SBA nodes .....	315
<b>DN configuration settings .....</b>	<b>317</b>
DN Ranges panel .....	318
DN Range panel .....	318
DN N6 interface settings .....	319
DN routes settings .....	320

<b>DN User Plane .....</b>	<b>321</b>
DN Stateless UDP Traffic .....	322
DN Data Traffic .....	324
DN Voice Traffic .....	326
DN Video OTT Traffic .....	337
DN DNS Server Traffic .....	340
DN Predefined Applications Traffic .....	343
DN Capture Replay .....	343
DN Synthetic .....	345
DN UDG .....	347
DN Throttling settings .....	349
<b>DNS Server configuration settings .....</b>	<b>350</b>
DNS Server Ranges panel .....	350
DNS Server Range panel .....	350
DNS Server Ndnsserver interface settings .....	351
DNS Server Traffic Flow settings .....	352
<b>EASDF configuration settings .....</b>	<b>355</b>
EASDF Ranges panel .....	355
EASDF Range panel .....	356
EASDF Node settings .....	357
EASDF Neasdf interface settings .....	357
EASDF N6 interface settings .....	360
EASDF UE routes settings .....	360
EASDF DNS Server Settings .....	361
EASDF Custom NF Services settings .....	362
<b>IMS configuration settings .....</b>	<b>364</b>
CSCF Range panel .....	364
CSCF N6 interface settings .....	366
CSCF AF Interface settings .....	367
CSCF UE routes settings .....	370
Media Function Range panel .....	370
<b>MME configuration settings .....</b>	<b>372</b>

MME Ranges panel .....	373
MME Range panel .....	374
MME Node settings .....	375
MME S11 Interface Settings .....	377
MME N26 Interface Settings .....	378
MME S1 Interface Settings .....	380
MME S6a Interface Settings .....	381
MME Diameter settings .....	384
<b>NEF configuration settings .....</b>	<b>386</b>
NEF Ranges panel .....	386
NEF Range panel .....	387
NEF Node Settings .....	388
NEF Nnrf interface settings .....	389
NEF Remote SBA Nodes .....	391
NEF Custom NF Services settings .....	393
<b>NRF configuration settings .....</b>	<b>395</b>
NRF Ranges panel .....	396
NRF Range panel .....	396
NRF Node settings .....	397
NRF Custom NF Services settings .....	398
NRF Nnrf interface settings .....	399
NRF Remote SBA Nodes .....	401
<b>NSSF configuration settings .....</b>	<b>403</b>
NSSF Ranges panel .....	404
NSSF Range panel .....	404
NSSF Node settings .....	405
Nnssf Interface Settings .....	406
Remote SBA nodes .....	409
NSSF Restricted NSSAIs .....	409
NSSF Network Slices .....	411
NSSF Configured NSSAI .....	412
<b>PCF/PCRF configuration settings .....</b>	<b>413</b>

PCF/PCRF Ranges panel .....	414
PCF Range panel .....	415
PCF Node settings .....	416
PCF Custom NF Services settings .....	418
PCRF Node settings .....	418
PCF service area restrictions .....	421
PCF Npcf interface settings .....	423
PCF remote SBA nodes .....	424
<b>RAN configuration settings .....</b>	<b>426</b>
gNodeB .....	427
gNodeB Ranges panel .....	428
gNodeB Range settings .....	433
gNodeB Node settings .....	434
gNodeB NSSAI settings .....	436
gNodeB N2 interface settings .....	437
gNodeB N3 interface settings .....	440
eNodeB .....	442
eNodeB Ranges panel .....	443
eNodeB Range Settings .....	447
eNodeB Node Settings .....	447
S1-U Interface Settings .....	449
S1-MME Interface Settings .....	450
Passthrough interface settings .....	453
<b>SBI Fuzzer configuration settings .....</b>	<b>455</b>
SBI Fuzzer Ranges panel .....	455
SBI Fuzzer Range panel .....	456
SBI Node Settings .....	457
SBI Fuzzer interface settings .....	459
SBI Fuzzer Target Node .....	461
<b>SCP configuration settings .....</b>	<b>463</b>
SCP Ranges panel .....	463
SCP Range panel .....	464

SCP Node Settings .....	465
SCP Nscp interface settings .....	465
SCP Remote SBA Nodes .....	468
<b>SEPP configuration settings .....</b>	<b>470</b>
SEPP Ranges panel .....	470
SEPP Range panel .....	471
SEPP Node Settings .....	472
SEPP Custom NF Services settings .....	473
SEPP Nsepp interface settings .....	473
SEPP Remote SBA Nodes .....	476
<b>SGW configuration settings .....</b>	<b>478</b>
SGW Ranges panel .....	479
SGW Range panel .....	480
SGW S1-U Interface Settings .....	481
SGW S5-C Interface Settings .....	482
SGW S5-U Interface Settings .....	483
SGW S11 Interface Settings .....	484
SGW DUT S11 Interface Settings .....	485
<b>SMF/PGW-C configuration settings .....</b>	<b>486</b>
SMF/PGW-C Ranges panel .....	487
SMF/PGW-C Range settings .....	488
SMF Node settings .....	489
SMF Custom NF Services settings .....	491
SMF N4/Sx interface settings .....	491
SMF Nsmf interface settings .....	493
SMF Gx Interface settings .....	496
SMF S5-c interface settings .....	499
SMF remote SBA nodes .....	500
SMF Uplink Paths settings .....	505
SMF Slice and UPF Mapping settings .....	506
SMF EAS Deploy Subscription settings .....	506
SMF EAS Procedures Settings .....	507

<b>SMSF configuration settings .....</b>	<b>509</b>
SMSF Ranges panel .....	509
SMSF Range panel .....	510
SMSF Node settings .....	511
SMSF Nsmsf interface settings .....	511
SMSF Remote SBA Nodes .....	514
<b>UDM/HSS configuration settings .....</b>	<b>518</b>
UDM/HSS Ranges panel .....	519
UDM/HSS Range panel .....	520
UDM Range Settings .....	521
UDM Settings .....	521
UDM Node Settings .....	522
UDM/HSS Custom NF Services settings .....	525
UDM Nudm Interface Settings .....	526
UDM Remote SBA Nodes .....	528
HSS Range Settings .....	530
HSS Settings .....	530
HSS Node Settings .....	531
HSS S6a Interface Settings .....	532
UDM and HSS Range Settings .....	534
UDM/HSS Custom NF Services settings .....	535
<b>UDR configuration settings .....</b>	<b>537</b>
UDR Ranges panel .....	537
UDR Range panel .....	538
UDR Node Settings .....	539
UDR Nudr interface settings .....	539
UDR Remote SBA Nodes .....	542
UDR Custom NF Services settings .....	542
<b>UPF/PGW-U configuration settings .....</b>	<b>544</b>
UPF/PGW-U Ranges panel .....	545
UPF/PGW-U Range panel .....	546
UPF Node settings .....	547

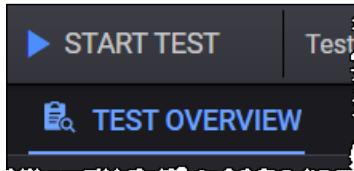
UPF N3 interface settings .....	547
UPF N4 interface settings .....	549
UPF N6 interface settings .....	550
UPF N9 interface settings .....	551
UPF Nupf Interface Settings .....	553
UPF N4u interface settings .....	554
UPF Remote SBA Nodes .....	556
UPF Slice Mapping settings .....	556
<b>5G-EIR configuration settings .....</b>	<b>558</b>
5G-EIR Ranges panel .....	558
5G-EIR Range panel .....	559
5G-EIR Node settings .....	559
5G-EIR N5g-eir interface settings .....	560
5G-EIR Remote SBA Nodes .....	562
<b>NF Discovery service .....</b>	<b>563</b>

## 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** ..... **122**

**Node Start/Stop Rates** ..... **122**

**DNS Settings** ..... **123**

**Advanced Settings** ..... **123**

**DNNs panel** ..... **127**

    DNN configuration settings ..... **129**

    Session AMBR configuration settings ..... **132**

    ePCO configuration settings ..... **133**

    Traffic Control Settings configuration ..... **134**

    3GPP RADIUS Server configuration ..... **135**

**Impairment** ..... **136**

**QoS Flows panel** ..... **137**

    QoS Flow configuration settings ..... **138**

    QoS Flow Packet Filter configuration settings ..... **141**

QoS Flow Max Packet Loss Rate settings .....	142
QoS Flow ARP configuration settings .....	142
QoS Flow MBR configuration settings .....	143
QoS Flow GBR configuration settings .....	143
<b>CA Certificates .....</b>	<b>143</b>
<b>Milenage .....</b>	<b>144</b>
<b>Customer Parameters .....</b>	<b>145</b>
<b>External Stats Server .....</b>	<b>145</b>
<b>Global Playlists .....</b>	<b>152</b>

## 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 <a href="#">Network Instance Format</a> .
<i>Links to detailed settings:</i>	
Node Start/Stop Rates	For more details, refer to <a href="#">Node Start/Stop Rates</a> .
DNS Settings	For more details, refer to <a href="#">DNS Settings</a> .
Advanced Settings	For more details, refer to <a href="#">Advanced Settings</a> .
DNNs	For more details, refer to <a href="#">DNNs</a> .
Impairment	For more details, refer to <a href="#">Impairment</a> .
QoS Flows	For more details, refer to <a href="#">QoS Flows</a> .
CA Certificates	For more details, refer to <a href="#">CA Certificates</a> .
Override Milenage Constants	For more details, refer to <a href="#">Milenage</a> .
Custom Parameters	For more details, refer to <a href="#">Custom Parameters</a> .
External Stats Server	For more details, refer to <a href="#">External Stats Server</a> .
Global Playlists	For more details, refer to <a href="#">Global Playlists</a> .
Secret Management System	For more details, refer to <a href="#">Secret Management System</a> .

### Node Start/Stop Rates

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

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

The DNS information is used only for the user plane path, that is, the configured DNS Server is used to resolve the destination configured for the user plane objectives in case the destination is a host name and not an IP.

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 <b>Add DNS Name Server</b> button to add a new DNS server to your test configuration. Set the IP address of the DNS server.
	Select the <b>Delete</b> button to remove the DNS server from your test configuration.

## Advanced Settings

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

Setting	Description
Overwrite	Enable this option to overwrite the capture size for IxStack.

Setting	Description
Capture Size	
Custom Capture Size	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.
Power Saver on Agents	Select this option to disable the IxStack/DPDK at the end of each test on all agents.
Enable Per UE Stats	Select this option to enable per UE statistics.
Enable per PDU Session Stats	Select this option to enable per PDU Session statistics.
Enable Per QoS Flow Stats	Select this option to enable per QoS Flow statistics.
Enable Control Plane Advanced Stats	Select this option to enable control plane latency statistics.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: <ul style="list-style-type: none"> <li>• <b>None</b> - no advanced statistics enabled.</li> <li>• <b>One Way Delay</b> - the time spent by the packet on the network from the moment it is sent until it is received.</li> <li>• <b>Delay Variation Jitter</b> - the per polling interval average delay variation jitter value calculated for all packets.</li> </ul>
Automated Polling Interval	This option is enabled by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval (sec)	This option becomes available only when <i>Automated Polling Interval</i> option is disabled. It allows you to create a custom polling interval.
Log Level	Select one of the options: <ul style="list-style-type: none"> <li>• <b>Info</b> - Designates informational messages that highlight the progress of the application at coarse-grained level.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>• <b>Debug</b> - Designates fine-grained informational events that are most useful to debug the application.</li> </ul>
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 Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.</p>
Traffic Settings	See <a href="#">Traffic Settings</a>
Response Cache	See <a href="#">Response Cache Settings</a> .
Ignore Offline Agents At Runtime	When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.

## Traffic Settings

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

Setting	Description
<i>GTPU Source Port:</i>	
Start	Indicates the source port for the GTPU tunnel. By default, the registered UDP port for GTPU is 2152.
Count	Set the count value.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable RTP.
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.
Enable Jumbo Frame	<p>Enable this option if your test traffic requires the use of jumbo frames (Ethernet frames with more than 1500 bytes of payload).</p> <p>When you enable this option, you can then configure any of the MTU parameters in the test to any valid jumbo frame size (up to 9,000 bytes).</p>

<b>Setting</b>	<b>Description</b>
Enable IxStack L4 Port Randomization	Select this option to enable IxStack L4 Port Randomization.
Enable UDP Port Recycling	Select this option to enable IxStack UDP Port Recycling.
Enable TCP Port Recycling	Select this option to enable IxStack TCP Port Recycling.
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).

## Response Cache Settings

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

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

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

<b>Setting</b>	<b>Description</b>
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.

## 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:

<b>DNN configuration settings</b> .....	<b>129</b>
<b>Session AMBR configuration settings</b> .....	<b>132</b>
<b>ePCO configuration settings</b> .....	<b>133</b>
<b>Traffic Control Settings configuration</b> .....	<b>134</b>
<b>3GPP RADIUS Server configuration</b> .....	<b>135</b>

## 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"> <li>• A mandatory Network Identifier that defines the external network to which the UPF is connected.</li> <li>• An optional Operator Identifier that defines the PLMN backbone in which the UPF is located.</li> </ul> <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><b>NOTE</b> 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"> <li>• <code>dnn[4-9,]</code> an implicit increment of 1 is used</li> <li>• <code>dnn[4-9]</code> as above</li> <li>• <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</li> <li>• <code>dnn[4-,]</code> as above</li> <li>• <code>dnn[4-]</code> as above</li> <li>• <code>dnn[4]</code> as above</li> </ul> <p>UEs will use the DNN values from the pool in a round robin manner.</p>

Setting	Description
	<p><b>IMPORTANT</b> If multiple sequence generators are configured and their pools overlap (for example: dnn[000-600,1].keysight.com dnn[500-999,1].keysight.com), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the start_value (they might start with an intermediate value in the second pool).</p>
PDU Type	Select the desired PDU type: IPv4, IPv6, IPv4v6 or Ethernet.
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 <a href="#">QoS Flow configuration settings</a>.</p>
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> <li>SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved.</li> <li>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.</li> <li>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.</li> </ul>
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

<b>Setting</b>	<b>Description</b>
	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.
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.
Include APN/DNN in PFCP Messages	<p>Enable this option to include APN/DNN in PFCP messages.</p> <p>By default, this option is disabled.</p>
Dual Registration Mode	When enabled, it transfers this session to the other RAT in dual registration mode. If the session does not exist, it will be created in the other RAT.
MPS Priority Level	Specify the Multimedia Priority Services (MPS) priority level. This is the relative priority level for MPS.
IMS Signaling Priority	Specify the IP Multimedia Subsystem (IMS) signaling priority. This value indicates subscription to IMS signaling priority service. The priority applies only to IMS signaling traffic.

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 <a href="#">Session AMBR configuration settings</a>.</i>
ePCO	<i>Select this option to open the extended protocol configuration options panel. These settings are described in <a href="#">ePCO configuration settings</a>.</i>
Traffic Control Settings	<i>Select this option to open the traffic control settings panel. These settings are described in <a href="#">Traffic Control Settings configuration</a>.</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

This 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.
EDC Support	If enabled, indicates that the UE has Edge DNS Client functionality. <b>IMPORTANT</b> This field becomes available only if the <b>Technical Spec Version</b> from Global Settings is set to <b>R17 December 2022</b> .
DNS Server IPv4 Address	If ePCO IE was received in PDU Session Establishment Request and DNS Server IPv4 Address Request was set, send this DNS IPv4 address in the ePCO IE in PDU Session Establishment Accept message if this field is not empty. <b>NOTE</b> The DNS Server IPv4 address will be replaced in the PDU Session Establishment Accept message if SMF learns dynamically a DNS IP address during EAS Discovery. <b>NOTE</b> If this field is empty and a DNS Name Server is configured in Global Settings > DNS Settings > <a href="#">DNS Name Servers</a> , then this field will be populated with the first IPv4 address of the DNS Name Server(s) defined in Global Settings.

Parameter	Description
	<p><b>NOTE</b> This value will be populated in the ePCO IE of the PDU Session Establishment Accept only if no other value is discovered by the SMF in the Multi-access Edge Computing (MEC) EAS Discovery procedure.</p>
DNS Server IPv6 Address	<p>If ePCO IE was received in PDU Session Establishment Request and DNS Server IPv6 Address Request was set, send this DNS IPv6 address in the ePCO IE in PDU Session Establishment Accept message if this field is not empty.</p> <p><b>NOTE</b> The DNS Server IPv6 address will be replaced in the PDU Session Establishment Accept message if SMF learns dynamically a DNS IP address during EAS Discovery.</p> <p><b>NOTE</b> If this field is empty and a DNS Name Server is configured in Global Settings &gt; DNS Settings &gt; <a href="#">DNS Name Servers</a>, then this field will be populated with the first IPv6 address of the DNS Name Server(s) defined in Global Settings.</p> <p><b>NOTE</b> This value will be populated in the ePCO IE of the PDU Session Establishment Accept only if no other value is discovered by the SMF in the Multi-access Edge Computing (MEC) EAS Discovery procedure.</p>
EDC Permission	<p>The SMF indicates, at PDU Session Establishment or at PDU Session Modification, that the use of the EDC is required or allowed for the PDU Session for the specific DNN. Available options are: <b>None</b>, <b>Allowed</b> or <b>Required</b>.</p> <p><b>IMPORTANT</b> This field becomes available only if the <b>Technical Spec Version</b> from Global Settings is set to <b>R17 December 2022</b>.</p>

Known limitations:

- 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.

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

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.

## 3GPP RADIUS Server configuration

The following tables describes the 3GPP RADIUS Server configuration parameters.

<b>Parameter</b>	<b>Description</b>
IP Address	The IP Address of the RADIUS Server used for this DNN. This IP Address will be used by the SMF <a href="#">3GPP RADIUS Client on page 490</a> to send 3GPP RADIUS messages to.
Authentication Port	The UDP port used by the RADIUS Server for the Authentication messages. This port will be used by the SMF <a href="#">3GPP RADIUS Client on page 490</a> to send Authentication messages to.
Accounting Port	The UDP port used by the RADIUS server for the Accounting messages. This port will be used by the SMF <a href="#">3GPP RADIUS Client on page 490</a> to send Accounting messages to.
Shared Secret	A text string that serves as a password between the RADIUS client and the RADIUS server.

Parameter	Description
Default Password	The default password used for PAP authentication when no password is received from the UE.

## Impairment

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

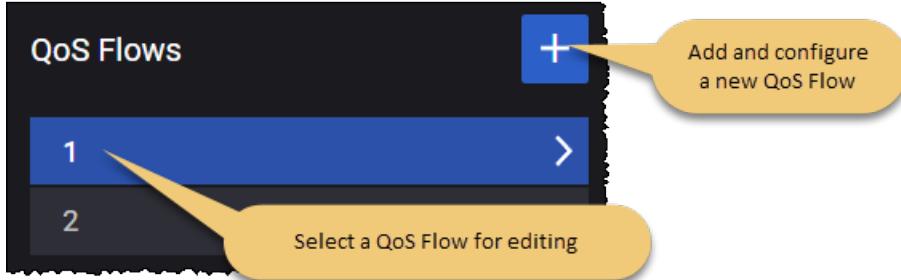
Setting	Description
<i>Impairment Profiles:</i>	
	Select the <b>Add impairment profile</b> button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete impairment profile</b> button to remove the profile from your test configuration.
Name	Each impairment profile 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"> <li>• Custom script</li> <li>• PFCP-drop message</li> </ul>
Script file	This parameter is available only when <b>Action Type</b> is set to <b>Custom script</b> . It allows you to add a custom script, using the <b>Upload</b> button. To remove the script, select the <b>Clear</b> 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:

<b>QoS Flow configuration settings</b>	<b>138</b>
<b>QoS Flow Packet Filter configuration settings</b>	<b>141</b>
<b>QoS Flow Max Packet Loss Rate settings</b>	<b>142</b>
<b>QoS Flow ARP configuration settings</b>	<b>142</b>
<b>QoS Flow MBR configuration settings</b>	<b>143</b>
<b>QoS Flow GBR configuration settings</b>	<b>143</b>

## 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><b>IMPORTANT</b> This parameter is available only if the <a href="#">Is Default</a> option is not selected.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Data</b> - 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.</li> <li>• <b>Audio</b> - LoadCorePCF/PCRF needs information related to this flow/bearer from CSCF.</li> <li>• <b>Video</b> - LoadCorePCF/PCRF needs information related to this flow/bearer from CSCF.</li> </ul>
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

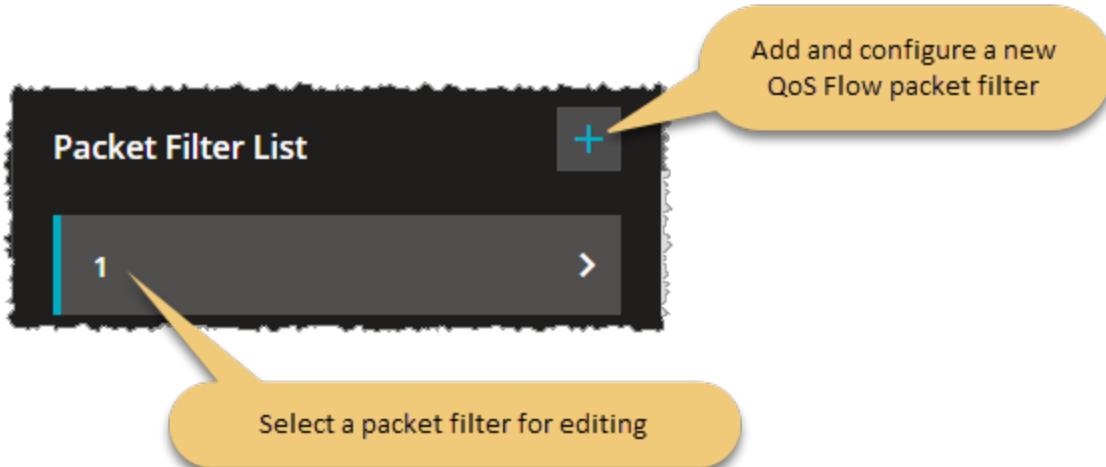
<b>Setting</b>	<b>Description</b>
Type	(GBR), Non-Guaranteed Bit Rate (non-GBR), or Delay Critical GBR. The Resource Type determines whether or not dedicated network resources related to a QoS Flow-level Guaranteed Flow Bit Rate (GFBR) value are permanently allocated to the flow.
Averaging Window	Specify 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	Specify the desired QoS Rule Precedence value for this QFI. The QoS rule precedence value (and the PDR precedence value) determine the order in which a QoS rule or a PDR, respectively, will be evaluated. The evaluation of the QoS rules or PDRs is performed in increasing order of their precedence value.
Packet Delay Budget	The Packet Delay Budget (PDB) defines an upper bound for the time that a packet may be delayed between the UE and the PCEF. For a given QCI, the value of the PDB is the same in uplink and downlink. The purpose of the PDB is to support the configuration of scheduling and link layer functions.
Packet Error Rate	The Packet Error Rate (PER) defines the upper bound for the rate of PDUs (IP packets) that have been processed by the sender of a link layer protocol but are not successfully delivered by the corresponding receiver to the upper layer. It defines an upper bound for the rate of non-congestion related packet losses.
Max Data Burst	The Maximum Data Burst Volume is the amount of data which the RAN is expected to deliver within the part of the Packet Delay Budget allocated to the link between the UE and the radio base station.
QoS Reference	This option is used on the PCF node to identify a particular PCC Rule when QoS reference information is received from the NEF on N33 interface. <b>NOTE</b> QoS Reference is supported only when Technical Spec Version is R16 or higher.
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	<b>IMPORTANT</b> This is available if <a href="#">Is Default</a> option is not enabled. If this option is not enabled, a new <a href="#">Packet Filter List</a> option appears and custom packet filter can be configured.
EPS Bearer	The EBI for the bearer associated with this QoS flow.

<b>Setting</b>	<b>Description</b>
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	<p>If needed, enable this option.</p> <p>This option is part of the Option 3x and Dual Connectivity NR feature, for more details refer to <a href="#">UE Range Panel</a>.</p>
Packet Filter List	<p><b>IMPORTANT</b> This is available if <a href="#">Use Match-all Packet Filter</a> option is not selected.</p> <p>Refer to the following topic for a description of the Packet Filter configuration settings: <a href="#">QoS Flow Packet Filter configuration settings on the facing page</a>.</p>
Max Packet Loss Rate	Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: <a href="#">QoS Flow Maximum Packet Loss configuration settings</a> .
ARP	Refer to the following topic for a description of the ARP configuration settings: <a href="#">QoS Flow ARP configuration settings</a> .
MBR	Refer to the following topic for a description of the MBR configuration settings: <a href="#">QoS Flow MBR configuration settings</a> .
GBR	Refer to the following topic for a description of the GBR configuration settings: <a href="#">QoS Flow GBR configuration settings</a> .

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

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

## **QoS Flow Max Packet Loss Rate settings**

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

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

## **QoS Flow ARP configuration settings**

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

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

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

## QoS Flow GBR configuration settings

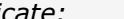
GBR indicates the guaranteed bit rates for service data flows that are mapped to this QoS flow. Separate GBR values are configured for uplink and downlink traffic.

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

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

## CA Certificates

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

Setting	Description
<p><i>CA Certificates:</i></p>	
	Select the <b>Add CA Certificate</b> button to add a new certificate to your test configuration.
<p><i>CA Certificate:</i></p>	
	Select the <b>Delete CA Certificate</b> 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 (.zip)	It allows you to add the certificate from the storage location, using the <b>Upload</b> button. You can upload a CA certificate in CRT or ZIP format that include multiple CA certificate files grouped in a folder.  To remove the file, select the <b>Clear</b> button.

# Milenage

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

Setting	Description
C4	<p>Set the C4 value (string type).</p> <p>Default value: <b>0004.</b></p>
R4	<p>Set the R4 value (integer type).</p> <p>Default value: <b>64.</b></p>
C5	<p>Set the C5 value (string type).</p> <p>Default value: <b>0008.</b></p>
R5	<p>Set the R5 value (integer type).</p> <p>Default value: <b>96.</b></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.

## External Stats Server

If this option is selected, it will allow you to add an external statistic server.

The following table describes the settings required for the External Stats Server configuration.

Setting	Description
<i>External Stats Server:</i>	
Profile	This parameter allows you to upload or remove a stats server profile. Press <b>Upload</b> and load the preferred server profile, or <b>Clear</b> to dismiss one that is set.
Server Address	The address of the external stats server.

## **Setting up a Profile**

The External Stats Server feature allows you to forward statistic logs to an external server, thus requiring to upload a profile that defines where the stats are stored and what stats should be transferred.

**IMPORTANT** This feature is designed to support any type of external entity, but currently it supports only the Apache Kafka Plugin.

The parameters required to create the request to the external entity are configured in the **Profile** JSON file that is uploaded to Keysight Open RAN Simulators, Cloud Edition 5.1. The following structure and parameters describe the standard content of the JSON file:

Section/ Parameter	Definition	Code Sample
<i>Input section</i>		<p><i>Lists all the stats/config parameters used in the profile. All the parameters are already available in Keysight Open RAN Simulators, Cloud Edition 5.1. the following types are supported:</i></p>
stat	<p>It can be any stat supported in Keysight Open RAN Simulators, Cloud Edition 5.1. The stats can be filtered by any other stat from the stat response.</p>	<p>With filter sample:</p> <pre data-bbox="804 487 1445 846"> {   "type": "stat",   "group": "AgentStatistics",   "stat": "CPU Percent",   "name": "cpu_percent1",   "filterBy": {     "stat": "agentIP",     "value": "10.38.158.83"   } } </pre> <p>Without filter sample:</p> <pre data-bbox="804 920 1445 1199"> {   "type": "stat",   "group": "Fullcoreoverview_RegisteredAttachedUE",   "stat": "UEs Registered",   "name": "no_of_UE_Registered" } </pre>
config	<p>It can be any parameter exposed in the UI. The path is the same as the one used by the UI to set/get a parameter (see <a href="#">Parameter sample path on the facing page</a> image).</p>	<pre data-bbox="804 1252 1445 1495"> {   "type": "config",   "group": "config/nodes/ausf/ranges/1/nodeSettings",   "stat": "mcc",   "name": "mcc" } </pre>
<i>Mappings section</i>		<p><i>Mapping will use any input parameter referred by name. Mapping also supports mathematical expressions to combine stats.</i></p>
	<p>For example, Keysight Open RAN Simulators, Cloud Edition 5.1 exposes <code>stat1</code> and <code>stat2</code> but the user needs <code>user_stat</code> which comprises (<code>stat1 +</code></p>	<ul style="list-style-type: none"> <li>• one parameter sample:</li> </ul> <pre data-bbox="804 1695 1445 1854"> {   "type": "controlplane",   "from": "no_of_UE_Registered",   "to": "no_of_UE_Registered" } </pre>

Section/ Parameter	Definition	Code Sample
	<p>stat2) /100. The expression is evaluated and the result sent under user_stat name.</p>	<pre data-bbox="806 318 1449 397">}</pre> <p>OR</p> <pre data-bbox="806 454 1449 671">{     "type": "controlplane",     "from": "mcc",     "to": "MCC" }</pre> <ul style="list-style-type: none"> <li>• with mathematical expression:</li> </ul> <pre data-bbox="806 749 1449 967">{     "type": "controlplane",     "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",     "to": "agent1 cpu ratio" }</pre>

## Parameter sample path



The screenshot shows a browser window with the URL <https://10.38.157.61/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings>. The page displays a JSON object representing node settings. The JSON structure includes fields like instanceId, mcc, mnc, routingIndicators, and links. The 'mcc' field is highlighted in red, indicating it's a parameter being discussed.

```

{
  instanceId: "7ea3abc7-f0f6-435b-9154-125deddd101b",
  mcc: "226",
  mnc: "04",
  - routingIndicators: [
      1234,
      2222
    ],
  - links: [
    - {
      rel: "self",
      type: "self",
      method: "GET",
      href: "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings"
    },
    - {
      rel: "meta",
      type: "meta",
      method: "GET",
      href: "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings/$options"
    }
  ]
}

```

## Sample profile

```

{
  "profile": {
    "type": "kafka",
    "3gpp_scenario": "QUIC_ABR_DEBUG",
    "event_type": "ATTS-TOOLS-KEYSIGHT-EVENT",
  }
}

```

```

    "specversion": "1.1",
    "kafkatopics": "com.att.ant.stage.ATTSSKeysight.1.0",
    "kafkaschemaUrl": "https%3A%2F%2Fc1001.eastus2.uat.iebus.3pc.att.com%3A8082%2Fschemas%2Fids%2F6635&schemaId=14260",
        "kafkaHeaderBootstrapUrl": "c1001.eastus2.uat.iebus.3pc.att.com:9093",
        "kafkaHeaderSaslMechanism": "PLAIN",
        "kafkaHeaderOAuthScope": "ANT-data-feed-dev-stage",
        "kafkaUsername": "m30317@ant.att.com",
        "kafkaPassword": "August2023#",
        "input": [
            {
                "type": "stat",
                "group": "AgentStatistics",
                "stat": "CPU Percent",
                "name": "cpu_percent1",
                "filterBy": {
                    "stat": "agentIP",
                    "value": "10.38.158.83"
                }
            },
            {
                "type": "stat",
                "group": "AgentStatistics",
                "stat": "CPU Percent",
                "name": "cpu_percent2",
                "filterBy": {
                    "stat": "agentIP",
                    "value": "10.38.157.97"
                }
            },
            {
                "type": "config",
                "group": "config/nodes/ausf/ranges/1/nodeSettings",
                "stat": "mcc",
                "name": "mcc"
            },
            {
                "type": "config",
                "group": "config/nodes/ue/ranges/1/userPlane/tigerObjective/1/statelessUDP",
                "stat": "ipAddress",
                "name": "ipAddress"
            },
            {
                "type": "stat",
                "group": "Fullcoreoverview_RegisteredAttachedUE",
                "stat": "UEs Registered",
                "name": "no_of_UE_Registered"
            },
            {

```

```

        "type": "stat",
        "group": "Fullcoreoverview_PDUSessionEstablishment",
        "stat": "PDU Session Establishment Succeeded",
        "name": "no_of_PDU_Session_Established"
    },
    {
        "type": "stat",
        "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
        "stat": "L2-3 Device Rx Traffic",
        "name": "L3 Server::Total Bits/Sec"
    },
    {
        "type": "stat",
        "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
        "stat": "L2-3 Device Tx Traffic",
        "name": "L3 Client::Total Bits/Sec"
    },
    {
        "type": "stat",
        "group": "Fullcoreapplicationtraffic_TCPConnections",
        "stat": "TCP connections established",
        "name": "HTTP/s Handshakes Succeeded"
    },
    {
        "type": "stat",
        "group": "Fullcoreapplicationtraffic_TCPConnections",
        "stat": "TCP connect failed",
        "name": "HTTP/s Handshakes Failed"
    },
    {
        "type": "stat",
        "group": "Fullcoreapplicationtraffic_TCPConnections",
        "stat": "TCP connections closed normally",
        "name": "HTTP/s Connection Closed"
    }
],
"mappings": [
    {
        "type": "controlplane",
        "from": "cpu_percent1 + cpu_percent2",
        "to": "total cpu_percent %"
    },
    {
        "type": "controlplane",
        "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",
        "to": "agent1 cpu ratio"
    },
    {
        "type": "controlplane",
        "from": "cpu_percent2/(cpu_percent1 + cpu_percent2)",
        "to": "agent2 cpu ratio"
    }
]
}

```

```

},
{
  "type": "controlplane",
  "from": "mcc",
  "to": "MCC"
},
{
  "type": "controlplane",
  "from": "ipAddress",
  "to": "Destination IP Address"
},
{
  "type": "controlplane",
  "from": "no_of_UE_Registered",
  "to": "no_of_UE_Registered"
},
{
  "type": "controlplane",
  "from": "no_of_PDU_Session_Established",
  "to": "no_of_PDU_Session_Established"
},
{
  "type": "userplane",
  "from": "L3 Server::Total Bits/Sec",
  "to": "L3 Server::Total Bits/Sec"
},
{
  "type": "userplane",
  "from": "L3 Client::Total Bits/Sec",
  "to": "L3 Client::Total Bits/Sec"
},
{
  "type": "userplane",
  "from": "HTTP/s Handshakes Succeeded",
  "to": "HTTP/s Handshakes Succeeded"
},
{
  "type": "userplane",
  "from": "HTTP/s Handshakes Failed",
  "to": "HTTP/s Handshakes Failed"
},
{
  "type": "userplane",
  "from": "HTTP/s Connection Closed",
  "to": "HTTP/s Connection Closed"
}
]
}
}

```

**Event body sent to Kafka**

```
[
  {
    "eventBody": {
      "id": "wireless-0acbc45b-8777-4250-a3ec-4f00e47399c8_39",
      "time": "2024-02-29T13:57:35Z",
      "type": "ATTS-TOOLS-KEYSIGHT-EVENT",
      "specversion": "1.1",
      "source": "https://10.38.157.61/wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
      "datacontenttype": "application/json",
      "payload": [
        {
          "type": "resource_info",
          "resource_info": {
            "simulated_tool_info": [
              {
                "tool_name": "LoadCore",
                "middleware_ip": "10.38.157.61"
              }
            ],
            "network_type": "5G",
            "3gpp_scenario": "QUIC_ABR_DEBUG"
          }
        },
        {
          "type": "test_execution_result",
          "test_execution_result": {
            "control_plane_result": {
              "Destination IP Address": "20.0.6.10",
              "MCC": "226",
              "agent1 cpu ratio": "0.455321",
              "agent2 cpu ratio": "0.544679",
              "no_of_PDU_Session_Established": "100",
              "no_of_UE_Registered": "0",
              "total cpu_percent %": "3.0902"
            },
            "userplane_plane_result": {
              "L3 Client::Total Bits/Sec": "0",
              "L3 Server::Total Bits/Sec": "0"
            }
          }
        },
        {
          "type": "test_execution_details",
          "test_execution_details": {
            "testName": "4 - Full Core Base Config",
            "testSessionID": "wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
            "UserID": "admin@example.org",
            "testStatus": "STOPPING",
            "testStartTime": "2024-02-29T13:55:40Z",
            "testDuration": 105,
          }
        }
      ]
    }
  ]
]
```

```

        "testStopTime": "2024-02-29T13:57:31Z"
    }
}
],
},
"payloadType": "JSON",
"value": {}
}
]

```

## Global Playlists

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

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

<b>UE Ranges panel</b>	<b>155</b>
<b>UE Range panel</b>	<b>156</b>
<b>Range Settings</b>	<b>158</b>
UE Identification settings	159
UE Security settings	159
UE Settings settings	163
UE Shared Data IDs	171
UE Subscribed AMBR settings	171
Service Area Restriction settings	171
Forbidden Areas	173
DNNs Config	174
Notifications	177
SMS Configuration	177
Equipment Status	180
Converged Charging	180
Spending Limit Control	181
Internal Group IDs	184
<b>Network Slicing settings</b>	<b>185</b>
UE NSSAI settings	186
UDM Default NSSAI settings	187
UDM SNSSAI Mappings	187
UDR SNSSAI Settings	188
<b>Objectives</b>	<b>189</b>
Control Plane Objective	190

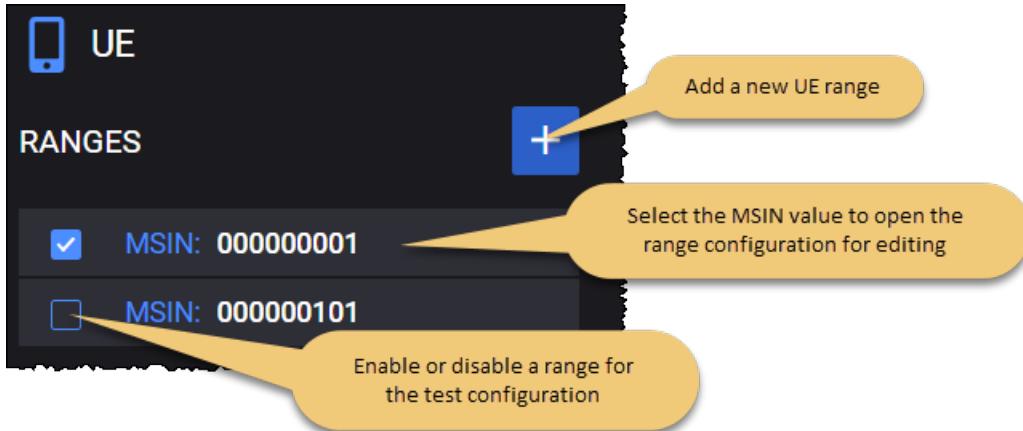
User Plane Objectives .....	206
-----------------------------	-----

## 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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All UE Ranges and RAN Ranges on All Agents** - on each agent a chunk of UEs from each UE range and a chunk of RANs from each RAN range will be configured.
- **Round Robin UE Ranges and RAN Ranges per Agent** - UE ranges will be distributed round-robin on the assigned agents, and chunks from RAN ranges will be distributed on the Agents, where the UE ranges from that Agents use the RAN nodes (either as Parent Node, or in the Handover, or EPS Fallback sections).

## UE Range panel

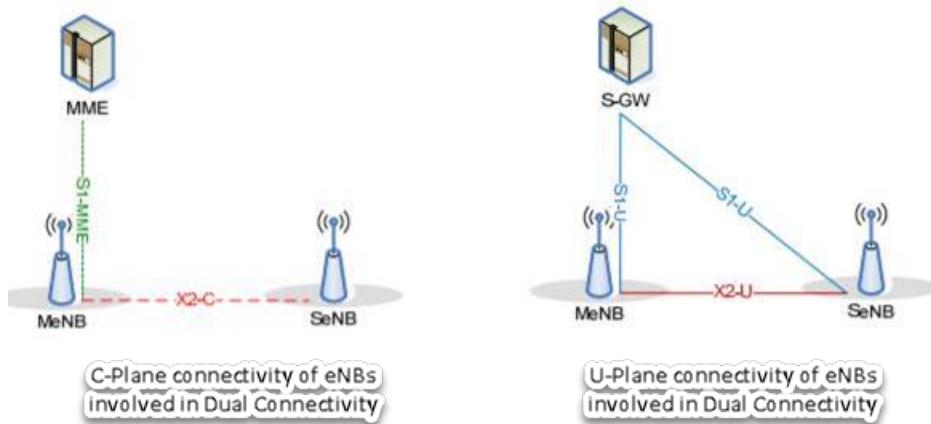
When you select an MSIN from the UE **Ranges** panel, LoadCore opens the **Range** panel, from which you can:

- 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 <b>Delete Range</b> 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:

<b>UE Identification settings</b> .....	<b>159</b>
<b>UE Security settings</b> .....	<b>159</b>
<b>UE Settings settings</b> .....	<b>163</b>
<b>UE Shared Data IDs</b> .....	<b>171</b>
<b>UE Subscribed AMBR settings</b> .....	<b>171</b>
<b>Service Area Restriction settings</b> .....	<b>171</b>
<b>Forbidden Areas</b> .....	<b>173</b>
<b>DNNs Config</b> .....	<b>174</b>
<b>Notifications</b> .....	<b>177</b>
<b>SMS Configuration</b> .....	<b>177</b>
<b>Equipment Status</b> .....	<b>180</b>
<b>Converged Charging</b> .....	<b>180</b>
<b>Spending Limit Control</b> .....	<b>181</b>
<b>Internal Group IDs</b> .....	<b>184</b>

## 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	<p>The MSIN value that will be assigned to the first simulated UE in the range.</p> <p><b>About MSIN ...</b></p> <p>The Mobile Subscriber Identification Number (MSIN) is a number that a wireless operator uses to uniquely identify a mobile phone. It is—at most—10-digits long. The MSIN is used (in combination with the MCC and MNC) to form the International Mobile Subscriber Identity (IMSI) number.</p>
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**.

<b>Setting</b>	<b>Description</b>
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.
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	The protection scheme used to generate the SUCI (for the purpose of

<b>Setting</b>	<b>Description</b>												
Scheme	<p>concealing the SUPI) for each UE in the range. The options are as follows:</p> <table border="1" data-bbox="437 325 1437 650"> <thead> <tr> <th data-bbox="442 331 556 361"><b>Scheme</b></th><th data-bbox="605 331 752 361"><b>Identifier</b></th><th data-bbox="801 331 1176 361"><b>Size of the scheme output</b></th></tr> </thead> <tbody> <tr> <td data-bbox="442 397 556 460">null-scheme</td><td data-bbox="605 397 654 426">0x0</td><td data-bbox="801 397 1405 460">Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)</td></tr> <tr> <td data-bbox="442 492 556 534">Profile-A</td><td data-bbox="605 492 654 521">0x1</td><td data-bbox="801 492 1405 555">Total of 256-bit public key, 64-bit MAC, and size of input</td></tr> <tr> <td data-bbox="442 587 556 629">Profile-B</td><td data-bbox="605 587 654 616">0x2</td><td data-bbox="801 587 1405 650">Total of 264-bit public key, 64-bit MAC, and size of input.</td></tr> </tbody> </table>	<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>	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.
<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>											
null-scheme	0x0	Size of the input (size of username used in case of NAI format or MSIN in case of IMSI)											
Profile-A	0x1	Total of 256-bit public key, 64-bit MAC, and size of input											
Profile-B	0x2	Total of 264-bit public key, 64-bit MAC, and size of input.											
Home Network Public Key	The home network public key that will be used for concealing the SUPI. The USIM stores the home network public key (if provisioned by the home operator).												
Home Network Public Key ID	The Home Network Public Key Identifier that will be used to indicate which public/private key pair to use for SUPI protection and deconcealment of the SUCI.												
Ephemeral Public Key	The ephemeral public key that will be used for computing a fresh SUCI on the UE side and for deconcealing the SUCI on the home network side.												
Ephemeral Private Key	The ephemeral private key that will be used for computing a fresh SUCI on the UE side.												
Routing Indicator	<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, <b>5G-AKA</b> 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"> <li>• <b>64 kbps</b></li> <li>• <b>Full Data Rate</b></li> </ul>												

Setting	Description
Integrity Protection Maximum Downlink Data Rate	Select a value from the drop-down list: <ul style="list-style-type: none"> <li>• <b>64 kbps</b></li> <li>• <b>Full Data Rate</b></li> </ul>
<i>UDM User Plane Security Profile</i>	<i>With this option you can configure User Plane security profiles. See <a href="#">UDM User Plane Security Profile below</a> table for details.</i>
<i>Override UE Security Capability</i>	<i>If selected, this option will override the default UE Security Capability settings. See <a href="#">Override UE Security Capability on the facing page</a> table for details.</i>

## UDM User Plane Security Profile

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

Parameter	Description
	Select the <b>Add Security Profile</b> button to add a new profile to your test configuration.
	Select the <b>Delete Profile</b> 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"> <li>• <b>REQUIRED</b></li> <li>• <b>PREFERRED</b></li> <li>• <b>NOT-NEEDED</b></li> </ul>
Confidentiality	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>REQUIRED</b></li> <li>• <b>PREFERRED</b></li> <li>• <b>NOT-NEEDED</b></li> </ul>

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.

## Override UE Security Capability

The following parameters are required to configure the Override UE Security Capability:

Parameter	Description
Include 5G UE Security Capabilities in 4G Attach	If enabled, the 4G Attach Request will contain the UE Additional Security Capability IE (5G UE Security Capability).
<i>5G Ciphering Algorithm</i>	<i>This section lists the supported 5G ciphering algorithm. By default, all settings are enabled. If required, you can disable each setting individually to avoid override.</i>
NEA0	Null ciphering algorithm (enabled by default).
NEA1	128-bit SNOW 3G based algorithm (enabled by default).
NEA2	128-bit AES based algorithm (enabled by default).
NEA3	128-bit ZUC based algorithm (enabled by default).
<i>5G Integrity Algorithm</i>	<i>This section lists the supported 5G integrity algorithm. By default, all settings are enabled. If required, you can disable each setting individually to avoid override.</i>
NIA0	Null ciphering algorithm (enabled by default).
NIA1	128-bit SNOW 3G based algorithm (enabled by default).
NIA2	128-bit AES based algorithm (enabled by default).
NIA3	128-bit ZUC based algorithm (enabled by default).

## UE Settings settings

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

Setting	Description
<i>Settings:</i>	
Dual Registration Mode	<p>When enabled, this option allows an UE to be registered/attached in the same time to 5GS via a gNodeB and to EPS via an eNodeB.</p> <p>The UE will activate this feature in case:</p> <ul style="list-style-type: none"> <li>• Dual Registration Mode option is enabled.</li> <li>• At least one DNN has <a href="#">Dual Registration Mode</a> option enabled.</li> <li>• It has a <a href="#">parent gNodeB</a> (<i>gNodeB-1</i> for example).</li> <li>• It has a Handover objective configured with <a href="#">visited nodes</a> (for example, primary node <i>gNodeB-1</i> and secondary node <i>eNodeB-1</i>).</li> </ul>

<b>Setting</b>	<b>Description</b>
	1).
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>
PCF Subscription to UDR	<p>Select the identifier that will determine the PCF to subscribe to UDR for AF-Traffic Influence events. Options are:</p> <ul style="list-style-type: none"> <li>• SUPI</li> <li>• Internal Grup ID</li> <li>• Any UE</li> </ul>
Set ESM Information Transfer Flag	<p>By default, this option is enabled.</p> <p>This option controls the value of the <i>ESM information transfer</i> flag from InitialUEMessage/AttachRequest 4G message.</p> <p>When this option is disabled, the UE/eNodeB will set the flag <i>ESM information transfer</i> to <i>False</i> and MME will not send DonwlinkNASTransport/ESM information request.</p>
Switch Off Deregistration/Detach	<p>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.</p>
PDU Session Release Before Deregistration	When this option is enabled, the UE will release PDU sessions before deregistration.
Enable Periodic Registration Update/Periodic	<p>By default, this option is not enabled.</p> <p>If the periodic registration / TAU functionality is disabled, the UE will</p>

<b>Setting</b>	<b>Description</b>
Tracking Area Update	<p>ignore the T3512/T3412 timer received in the Registration Accept/TAU Accept and will not send any Periodic Registration Update/Tracking Area Update request.</p> <p>During the Initial Registration/Initial Attach, the AMF/MME sends in the Registration Accept/Attach Accept a T3512/T3412 timer, which consists of a Unit-Value pair. For example, a value of 30 and unit of 10min means 300 minutes.</p> <p>The T3512/T3412 timer can be overridden by subsequent Registration Accept/TAU Accept messages. If T3512/T3412 is 0 or Disabled, no periodic registration/periodic TAU should be performed. If no T3512/T3412 value is present in the Registration Accept /Attach Accept message, the last known T3512/T3412 value is used. If a T3512/T3412 was never transmitted by the AMF/MME, the default value of 54 minutes will be used.</p> <p>The T3512/T3412 timer is triggered when the UE enters idle. If the UE exits the idle state, the T3512/T3412 timer is stopped. When the UE enters again in idle, the T3512/T3412 timer is restarted.</p> <p>While the UE is in idle mode, when the T3512/T3412 timer expires:</p> <ul style="list-style-type: none"> <li>• If the UE is not registered/attached for emergency services, the UE initiates a Periodic Registration Update/Tracking Area Update procedure and restarts the T3512/T3412 timer.</li> <li>• If the UE is registered/attached for emergency services, the UE locally de-registers/detaches and the AMF/MME locally detaches the UE.</li> </ul>
Include UEContextRequest IE for PRU Initial UE Message	<p>If enabled, it will include the UEContextRequest IE for the PRU Initial UE Message.</p> <p><b>IMPORTANT</b> This option appears only if <b>Enable Periodic Registration Update/Periodic Tracking Area Update</b> is enabled.</p>
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 Router Solicitation (ms)	The time (in milliseconds) that will elapse before the UE sends an ICMPv6 Router Solicitation message (a <b>0</b> value means no delay). If, during this time, the UE receives an unsolicited Router Advertisement, the sending of the Router Solicitation will be canceled.
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.
Check AUTN	By default, this option is disabled.

<b>Setting</b>	<b>Description</b>
	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.
AMF Force Identification During Registration	This option will force the AMF to always trigger the "Identification Procedure" to get the identity of the UE. When the NG-RAN node receives this request, it responds with the IMEISV or the SUCI.
Send Registration Accept in Initial Context Setup Request	If enabled, the UE will send Registration Accept in Initial Context Setup Request.
Always Include Uplink Data Status IE in Service Request Message	The UE will always include the Uplink Data Status IE for a Service Request message, not only if it has pending data.
Enable Passthrough	Select this option to enable passthrough and any interface. Applicable to all passthrough topologies (UE/gNB or UPF). Applicable to either direction: GTPu to IP or/and IP to GTPu.
Attach/Register with GUTI	When the Primary Objective type is Subscribers Per Second, enabling this option will trigger a Registration/Attach Request with the type of user identity set to temporary identity (GUTI). When option is not enabled, the type of user identity in the Registration/Attach Request will be permanent identity.
Authentication with GUTI	This option is available only when Attach/Register with GUTI option is enabled. When enabled, this option triggers authentication in case of attach (4G)/register (5G) with GUTI.
Force Emergency Registration	When this option is enabled, the UE will perform an Emergency registration (instead of Initial Registration). Only the primary objective's DNNs are taken into account when deciding if the UE performs an emergency registration. When the dnnIdsToActivate 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.
Identity Type for Emergency Registration	Select the identity type to use from the drop-down list. Available options are: <ul style="list-style-type: none"> <li>• <b>SUCI/IMSI</b> - where SUCI is used for 5G network, and IMSI for 4G network</li> <li>• <b>IMEISV/IMEI</b> - where IMEISV is used for 5G network, and IMEI</li> </ul>

<b>Setting</b>	<b>Description</b>
	<p>for 4G network.</p> <ul style="list-style-type: none"> <li>• <b>IMEI</b> - where IMEI is used for 5G networks</li> </ul>
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)	<p>The time that will elapse before indirect forwarding cleanup. The delay is calculated from the UE Context Release.</p>
Send Native GUTI During IRAT Mobility Registration	<p>Enable this option to send native GUTI during IRAT mobility registration.</p>
Authentication During Mobility Registration	<p>Select a value from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Never</b>: Authentication is not performed during mobility registration.</li> <li>• <b>Always</b>: Authentication during mobility registration is always performed.</li> <li>• <b>No Native Context</b>: Authentication during mobility registration is performed only when the UE does not hold a native 5G security context.</li> </ul>
Access Class	<p>Select the Access Class of the UE from the drop-down list. The following options are available: <i>None</i>, <i>Low Priority Access</i>, <i>11 - For PLMN Use</i>, <i>12 - Security Service</i>, <i>13 - Public Utilities</i>, <i>14 - Emergency Services</i>, <i>15 - PLMN Staff</i>.</p> <p><b>IMPORTANT</b> This option is available for 4G only.</p>
<i>Radio Capability</i>	
UE Radio Capability IE Value for LTE	<p>The UE radio capability IE value that will be included UE Capability Info Indication message.</p>
UE Radio Capability IE Value for NR	<p>The UE radio capability IE value that will be included UE Capability Info Indication message.</p>
Send UE Capability IE Indication after Initial Context Setup	<p>Select this option to sent UE capability IE indication after initial context setup.</p>
Replay UE Radio Capability	<p>The UE Radio Capability IE is replayed in the Initial Context Setup Request on 5G. This option is applicable for the AMF node only.</p>

Setting	Description
	<p><b>NOTE</b> It is not applicable for Initial Context Setup Request of an inter-RAT handover procedure.</p>
<i>Location Reporting</i>	<i>Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).</i>
Reporting Type	<p>Select the value from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Direct</b> - If the test timeline is long enough, the AMF generates <math>n</math> <code>LocationReportingControl</code> messages at every <math>m</math> seconds from the moment Registration Complete message is received by the AMF (<math>n</math> is the value configured for <a href="#">Number of Repeats</a> and <math>m</math> is the value of <a href="#">Interval Between Requests</a>).</li> <li>• <b>Change of Serving Cell</b> - In case of Handover with AMF change, if <b>Change of Serving Cell</b> is selected, after handover, the new AMF will send a <code>LocationReportingControl</code> message to the NG-RAN.</li> </ul>
Interval Between Requests (seconds)	Set the time interval between requests.
Number of Repeats	Set the number of repeats.
Start Time (seconds)	The number of seconds after successful attach when the AMF sends a <code>LocationReportingControl</code> message (event-type: <code>change-of-serv-cell</code> ).
Stop Time (Seconds)	The number of seconds since the <a href="#">Start Time</a> when the AMF sends <code>LocationReportingControl</code> message (event-type: <code>stop-change-serving-cell</code> ).
<i>Core Network Assistance Information For Inactive</i>	<p><i>If enabled, the configured Core Network Assistance Information for RRC INACTIVE IE is present only in the INITIAL CONTEXT SETUP REQUEST message carrying the initial Registration Accept. It is not present in the INITIAL CONTEXT SETUP REQUESTS carrying other types of NAS messages, UE CONTEXT MODIFICATION REQUEST, HANDOVER REQUEST or PATH SWITCH REQUEST ACKNOWLEDGE. It is not present for Emergency Registration.</i></p> <p><i>This option is disabled by default. See <a href="#">Core Network Assistance Information For Inactive</a> for configuration details.</i></p>
<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>

<b>Setting</b>	<b>Description</b>
	Applicable to simulated UDR NF.
<i>Operator Specific Data</i>	
<i>Policy data</i>	<i>This option allows for specific operator data to be added.</i>
<i>Use Operator Specific Data</i>	Enable this option to use operator specific data. A list of objects similar with the reconfigured example is expected.
<i>Operator Specific Data Policy JSON</i>	<p>Paste the operator specific data in JSON format into the field. Format and save the JSON content by selecting the <b>Save JSON</b> button.</p> <p>Default format:</p> <pre data-bbox="535 692 915 1660"> {     "opSpecDataName1": {         "dataType": "string",         "value": "aaaaa"     },     "opSpecDataName2": {         "dataType": "object",         "value": {             "member1": 1,             "member2": "string",             "member3": null         }     },     "opSpecDataName3": {         "dataType": "integer",         "value": 1023     },     "opSpecDataName4": {         "dataType": "array",         "value": [             {                 "member1": 1,                 "member2": "string",                 "member3": null             },             1025,             "another string"         ]     } } </pre>

## Core Network Assistance Information For Inactive

<b>Setting</b>	<b>Description</b>
	<i>Core Network Assistance Information For Inactive</i>

<b>Setting</b>	<b>Description</b>
UE Specific DRX	<p>The UE Specific DRX value can be selected from the available options:</p> <ul style="list-style-type: none"> <li>• <b>DRX32</b></li> <li>• <b>DRX64</b> (default value)</li> <li>• <b>DRX128</b></li> <li>• <b>DRX256</b></li> <li>• <b>None</b> - if selected, this IE will not be included in the message</li> </ul>
Include MICO Mode Indication	<p>Indicates if the UE is configured with MICO Mode by the AMF. If disabled, this IE will not be included in the message.</p>
<i>Expected UE Behaviour</i>	
Expected Handover Interval	<p>The expected time interval between inter NG-RAN node handovers. When set to <b>None</b>, this IE will not be included in the message. Select a value from the drop-down:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)</li> <li>• <b>Sec15</b></li> <li>• <b>Sec30</b></li> <li>• <b>Sec60</b></li> <li>• <b>Sec90</b></li> <li>• <b>Sec120</b></li> <li>• <b>Sec180</b></li> <li>• <b>Long Time</b></li> </ul>
Expected UE Mobility	<p>Indicates whether the UE is expected to be stationary or mobiles. When set to <b>None</b>, this IE will not be included in the message. Select a value from the drop-down:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)</li> <li>• <b>Stationary</b></li> <li>• <b>Mobile</b></li> </ul>
<i>Expected UE Activity Behaviour</i>	
Expected Activity Period	<p>The expected activity time in seconds. Any period longer than 180 seconds is represented by the value 181. When left empty, this IE will not be included in the message.</p>
Expected Idle Period	<p>The expected idle time in seconds. Any period longer than 180 seconds is represented by the value 181. When left empty, this IE will not be included in the message.</p>
Source Of UE Activity Behaviour	<p>Indicates the source of the UE activity behavior. When set to 'None' this IE will not be included in the message.</p>

Setting	Description
Information	Select a value from the drop-down: <ul style="list-style-type: none"> <li>• <b>None</b> (default)</li> <li>• <b>Subscription Information</b></li> <li>• <b>Statistics</b></li> </ul>

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

## 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 <b>Not Allowed Areas</b> or <b>Allowed Areas</b>.</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 <b>Add Area</b> button to add a new restriction area to your configuration.
<i>Area:</i>	
	Select the <b>Delete Area</b> 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 <b>Add TAC</b> button to add a new TAC to your configuration.</p> <p>Each <b>Area</b> 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</p>

Setting	Description
	construction of the Tracking Area Identity (TAI).
	Select the <b>Delete</b> 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 <b>Delete Forbidden Area</b> 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 <b>Delete</b> button to remove this TAC from your configuration.
TAC	<p>Each <b>Area</b> 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 <b>Add DNNs Config</b> button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the <b>Delete DNN Config</b> 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"> <li>SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved.</li> <li>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.</li> <li>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.</li> </ul>
Session ID	Provide the session ID value.
Alternate Session ID	<p><b>IMPORTANT</b> This parameter becomes available only if <b>SSC Mode</b> is set to <i>SSC Mode 2</i> or <i>SSC Mode 3</i>.</p> <p>Provide an alternate session ID value.</p>
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>

<b>Setting</b>	<b>Description</b>
	<p><b>NOTE</b> The reactivation delay is deactivated if an IRAT mobility occurs before the timer expires.</p>
Default Bearer Lifetime (s)	The time to wait before doing a network initiated delete for the default bearer for this APN. A zero value means this feature is disabled.
DNN	Select one of the previously-defined DNNs from the drop-down list.
Local IPv4 Address	<p>The IPv4 address that the UE receives from the SMF during PDU Session Establishment. This address is used for L4-7 traffic (source IP for the UL traffic, destination IP for the DL traffic). It is used only when LoadCoresimulates the SMF.</p> <p>IP address is also used to create UE Routes from DN.</p>
Local IPv4 Address Increment	The value by which the IP addresses will be incremented.
Local IPv4 Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Local IPv6 Address	<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	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Ethernet Device Information	<p>Allows adding multiple ethernet devices per DNN with PDU type Ethernet.</p> <p><b>NOTE</b> This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</p>
Ethernet PDU config	For each ethernet device the MAC Address, IP Address, outer VLAN and inner VLAN can be configured.
Enable TSN	<p>This feature is available only for spec version newer (including) Release 16 and Ethernet PDU type sessions.</p> <p><b>NOTE</b> This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</p>
DS-TT Ethernet Port MAC Address	The device-side TSN translator port MAC address.
Configure S-NSSAI:	<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,</i>

Setting	Description
	<p><i>the first slice from Allowed NSSAI list (received in Registration Accept) is used in PDU Session Establishment message.</i></p> <p><b>NOTE</b> <i>This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</i></p>
S-NSSAI	This list contains all the slices defined for the selected UE range. Select from the drop-down list the slice to be used in PDU Session Establishment.
Force S-NSSAI	<p>This option is used to control the behavior in case you select a slice that is not part of Allowed NSSAI received from AMF, as follows:</p> <ul style="list-style-type: none"> <li>if the checkbox is not selected, the UE will not send any slice in PDU Session Establishment message (as the slice selected from the above list is not part of Allowed NSSAI).</li> <li>if the checkbox is selected, the UE will use the slice selected from the above list, although it is not part of Allowed NSSAI.</li> </ul> <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"> <li><b>None</b></li> <li><b>EAP-TTLS</b> (Extensible Authentication Protocol – Tunnelled Transport Layer Security)</li> <li><b>CHAP</b> (Challenge-Handshake Authentication Protocol)</li> <li><b>PAP</b> (password Authentication Protocol)</li> </ul>
<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"> <li><b>PAP</b></li> <li><b>CHAP</b></li> </ul>
User	Provide the user.
Password	Provide the password.
Send User Identity	<p>By default, this option is disabled.</p> <p>Enabling this option will add SM PDU DN Request Container IE (Authentication Identity) to the PDU Session Establishment Request message send by NG-RAN.</p>
<i>Chap Auth Method:</i>	

<b>Setting</b>	<b>Description</b>
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.

<b>Setting</b>	<b>Description</b>
<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.

<b>Setting</b>	<b>Description</b>
<i>Mobile Settings:</i>	
Service Center Address	The service center address used by the UE range for SMS messaging.

<b>Setting</b>	<b>Description</b>
Type of Number	<p>The type of number can be one of the following:</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• International number</li> <li>• National number</li> <li>• Network specific number</li> <li>• Subscriber number</li> <li>• Alphanumeric</li> <li>• Abbreviated number</li> <li>• Reserved number</li> </ul>
Numbering Plan Identification	<p>The numbering plan identification can be one of the following:</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• ISDN</li> <li>• Data numbering plan</li> <li>• Telex numbering plan</li> <li>• National numbering plan</li> <li>• Private numbering plan</li> <li>• ERMES numbering plan</li> <li>• Reserved numbering plan</li> </ul>
Character Set	<p>The character set used in the data coding scheme for the text message.</p>
Text Message	<p>The content of text message sent by the UE via SMS.</p>
Mobile Terminate SMS Delay (s)	<p>The time in seconds to wait, after the UE registers, for the AMF or SMF to initiate an MT SMS.</p>
<i>SMS Configuration:</i>	
SMS Mode	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>SMS-MO:</b> Mobile Originated. The UE range originates (sends) SMS messages.</li> <li>• <b>SMS-MT:</b> Mobile Terminated. The UE range waits for delivery of SMS messages.</li> </ul>
Enable SMS Management Subscription Get	<p>This option has effect only for technical specification Release 16. If active (default), TS 23.502 <i>Registration procedures for SMS over NAS</i> step 7b (<code>Nudm_SDM_Get</code>) is performed.</p>
<i>SMS Management Subscription Data:</i>	

<b>Setting</b>	<b>Description</b>
SMS Management Subscription Data	<p>When selected, this pane displays the following options:</p> <ul style="list-style-type: none"> <li>• <b>Subscribed for MT SMS</b> - by default, this option is enabled.</li> <li>• <b>Barred All MT SMS</b> - by default, this option is disabled.</li> <li>• <b>Barred Roaming MT SMS</b> - by default, this option is disabled.</li> <li>• <b>Subscribed for MO SMS</b> - by default, this option is enabled.</li> <li>• <b>Barred All MO SMS</b> - by default, this option is disabled.</li> <li>• <b>Barred Roaming MO SMS</b> - by default, this option is disabled.</li> </ul> <p>If technical specification Release 16 is configured in <a href="#">Global Settings</a>, the <b>Trace Data</b> option is enabled.</p>

The following table describes the **Trace Data** settings.

<b>Setting</b>	<b>Description</b>
<i>Trace Data</i>	<i>Select the check box to enable this option.</i>
Trace Reference	<p>The trace reference string should be formed as follows: the concatenation of MCC, MNC and Trace ID as follows: &lt;MCC&gt;&lt;MNC&gt;&lt;Trace ID&gt;.</p> <p>This field cannot be empty.</p>
Trace Depth	<p>Select an option from the drop-down list: <b>MINIMUM</b>, <b>MEDIUM</b>, <b>MAXIMUM</b>, <b>MINIMUM_WO_VENDOR_EXTENSION</b>, <b>MEDIUM_WO_VENDOR_EXTENSION</b>, <b>MAXIMUM_WO_VENDOR_EXTENSION</b>.</p> <p>Default value: <b>MEDIUM</b>.</p>
NE Types	<p>Configures a hexadecimal number as string, i.e. only values 0-9, a-f are allowed.</p> <p>Default value: <b>000008</b>.</p> <p>This field cannot be empty.</p>
Triggering Events	<p>Configures a hexadecimal number as string, i.e. only values 0-9, a-f are allowed.</p> <p>Default value: <b>0000</b>.</p> <p>This field cannot be empty.</p>
Trace Collection Entity IPv4 Address	<p>Provide the IPv4 address. Default value: <b>192.168.0.1</b>.</p>
Trace Collection Entity IPv6 Address	<p>Provide the IPv6 address. Default value: empty.</p>
List of Interfaces	<p>Configures a hexadecimal number as string, i.e. only values 0-9, a-f are allowed.</p> <p>Can be empty. Default value: empty.</p>

## 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 <b>Add Blocked Subscribers</b> button to add a new range of blocked IMEIs.
	Select the <b>Delete Blocked Subscribers</b> 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 <b>Add Greylisted Subscribers</b> button to add a new range of greylisted IMEIs.
	Select the <b>Delete Greylisted Subscribers</b> 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-

<b>Setting</b>	<b>Description</b>
	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.
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.

<b>Setting</b>	<b>Description</b>
Enable Notify Timer	Use this option to enable the notify timer.
Trigger Notify	The time interval (in milliseconds) after which CHF will notify PCF with modified

Setting	Description
Timer (ms)	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 <a href="#">here</a>.</i>
Notify Policy Counters	<i>These settings are described <a href="#">here</a>.</i>

## Policy Counters

Applicable to simulated CHF Network Function. The following table describes the **Policy Counters** settings.

Setting	Description
<i>Policy Counters:</i>	
	Select the <b>Add Policy Counter</b> button to add a policy counter to your test configuration.
<i>Policy Counter settings:</i>	
	Select the <b>Delete Policy Counter</b> 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 <b>Add Pending Status</b> button to add a pending policy counter status.

Setting	Description
<i>Pending Policy Counter Status settings:</i>	
	Select the <b>Delete Pending Policy Counter Status</b> 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 <b>Add Policy Counter</b> button to add a policy counter to your test configuration for which you want to receive notifications.
<i>Policy Counter settings:</i>	
	Select the <b>Delete Policy Counter</b> 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 <b>Add Pending Status</b> button to add a pending policy counter status.
<i>Pending Policy Counter Status settings:</i>	
	Select the <b>Delete Pending Policy Counter Status</b> button to remove the pending policy counter status.
Policy	Enter the policy counter status (as a string value). For example: <i>120Mbps</i> .

Setting	Description
Counter Status	
Activation Time	Enter the activation time (as a DateTime value) for this status value. For example: 2020-12-31 11:59:59.

## Internal Group IDs

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

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

<b>UE NSSAI settings</b> .....	<b>186</b>
<b>UDM Default NSSAI settings</b> .....	<b>187</b>
<b>UDM SNSSAI Mappings</b> .....	<b>187</b>
<b>UDR SNSSAI Settings</b> .....	<b>188</b>

## 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 <b>Add UE NSSAI</b> button to add a new UE NSSAI to your test configuration.								
<i>UE NSSAI settings:</i>									
	Select the <b>Delete UE NSSAI</b> 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 <b>Add UDM Default NSSAI</b> button to add the default NSSAI to your test configuration.
<i>UDM Default NSSAI settings:</i>	
	Select the <b>Delete UDM Default NSSAI</b> 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 <b>Add SNSSAI Mapping</b> button to add the NSSAI mapping to your test configuration.
<i>UDM SNSSAI Mapping settings:</i>	

Setting	Description
	Select the <b>Delete SNSSAI Mapping</b> 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 <b>Add SNSSAI Settings</b> button to add the SNSSAI settings to your test configuration.
<i>UDR Settings:</i>	
	Select the <b>Delete SNSSAI Settings</b> 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:

<b>Control Plane Objective .....</b>	<b>190</b>
<b>User Plane Objectives .....</b>	<b>206</b>

## 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>	$20000 / 1000 = 20\text{s}$ 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.

<b>Phase</b>	<b>Activity during this phase</b>
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"> <li><b>Active Subscribers:</b> 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.</li> <li><b>Subscribers Per Second:</b> The test attempts to activate a specified number of subscriber sessions per second, within the rate and time parameters that you configure.</li> </ul> <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 <b>DNNs Config</b> Range settings.)</p> <p>The choices are:</p>

Parameter	Description
	<ul style="list-style-type: none"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> <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 <a href="#">DNNs panel</a> for more information.</p>
Number of Retries	<p>This value indicates how many times UE/NRAN 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"> <li>• <b>-1</b> : infinite retries for entire sustain time.</li> <li>• <b>0</b> (default value) : the retry option is disabled.</li> <li>• <b>1 to 127</b>: the number of retries per UE (Register + PDU Session procedure).</li> </ul>
<i>Subscribers Per Second:</i>	
Hold Time (s)	The number of seconds that each subscriber session will remain active. This is, therefore, the amount of time that will elapse between the subscriber attach and the subscriber detach. At the end of the session hold time, the subscriber performs the detach procedure.
Rate	The number of subscriber sessions to activate per second.
Sustain Time (s)	The duration of time (in Seconds) that the specified session activation rate will be maintained.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the <b>DNNs Config</b> Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> <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 <a href="#">DNNs panel</a> for</p>

Parameter	Description
	more information.

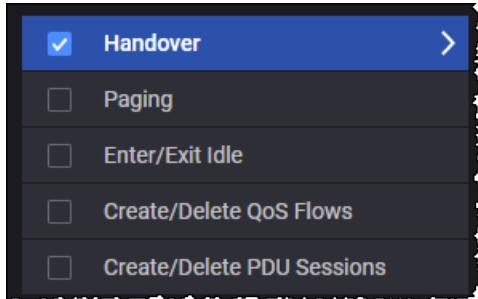
## Secondary Control Plane Objective

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:

<b>When the primary objective is:</b>	<b>then the secondary objectives will start...</b>
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 and Idle mode on RAN only (not supported in 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), <a href="#">Force S1 / N2 Handover</a> 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:

- .
- 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>	

Parameter	Description
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which handovers are initiated, measured in procedures per second if <b>Distributed over (s)</b> 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"> <li>• <b>Connected</b></li> <li>• <b>Idle</b></li> <li>• <b>Any</b></li> </ul> When <b>Any</b> 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"> <li>• <b>None</b> - 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.</li> <li>• <b>Connected</b> - The UE will perform Connected Handover from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that <b>if the UE was in idle state</b> before performing this mobility, the UE will <b>first perform exit idle</b>, and only after the UE is in connected state, will it initiate <b>the connected handover</b> to the parent RAN.</li> <li>• <b>Idle</b> - 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 <b>connected</b> state before performing this mobility, the UE will <b>first perform enter idle</b>, and only after the UE is in idle state, will it initiate the <b>idle mode mobility</b> to the parent RAN.</li> </ul>
Send Service Request after Returning to	By default, this option is disabled. Send Service Request immediately after Return to Parent Node Mobility if UE State was idle.

Parameter	Description
Parent Node	
<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"> <li>• <b>Connected</b></li> <li>• <b>Idle</b></li> <li>• <b>Any</b></li> </ul>
Primary Node	Select the primary node from the drop-down list.
Secondary Node	Select the secondary node from the drop-down list.
Send Service Request After Mobility	By default, this option is disabled. Send Service Request immediately after Mobility if UE State was idle.

## Paging

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

The following table describes the Paging objective parameters.

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

Parameter	Description
	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"> <li>If the UPF is the DUT in the test topology, then set the <i>Remote IP Address</i> to the DN IP address.</li> <li>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.</li> </ul>

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.

Parameter	Description
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds 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

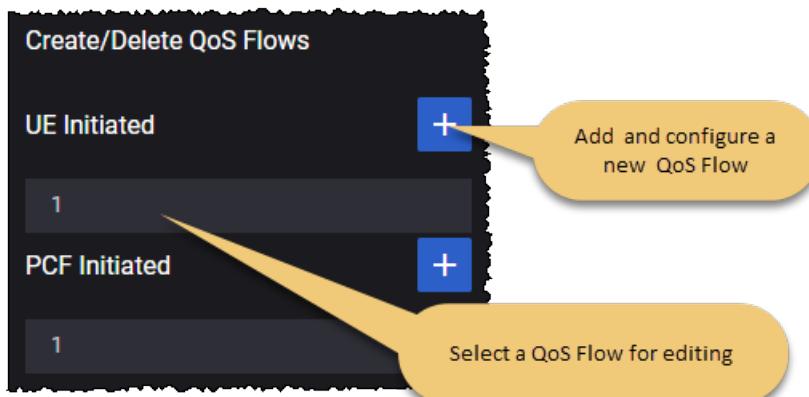
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured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

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

### Support for Network Initiated QoS Flow modification

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

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

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

## Notes:

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

## Create/Delete PDU Sessions

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

The following table describes the objective parameters.

Parameter	Description
<i>Create/Delete PDU Sessions:</i>	
	Select the <b>Add Objective</b> button to add an instance of this objective.
<i>Objective:</i>	
	Select the <b>Delete Objective</b> 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	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 <b>DNNs Config</b> Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> <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 <b>DNNs Config</b> 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.

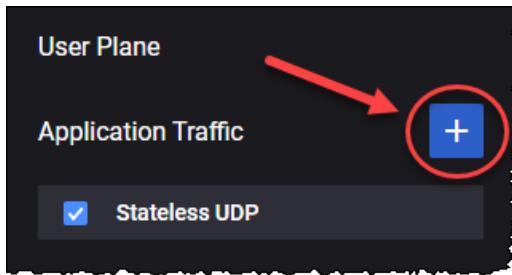
Parameter	Description
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	<p>The rate at which procedures are initiated, measured in procedures initiated per second.</p> <p>Using higher values for this parameter requires a large number 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	The increment for the destination MSISDN.

Parameter	Description
Increment	

## 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, Ping, Synthetic and UDG**.

**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"><li>• <b>Attacks</b></li><li>• <b>Stateless UDP</b></li><li>• <b>Data</b></li><li>• <b>Voice</b></li><li>• <b>Video OTT</b></li><li>• <b>DNS Client</b></li><li>• <b>Predefined Applications</b></li><li>• <b>Synthetic</b></li><li>• <b>UDG</b></li><li>• <b>Attacks</b></li></ul>
	Select this button to remove the application traffic objective from your test configuration.
Attacks	For the settings required to configure the Attacks traffic objective, refer to <a href="#">Attacks Traffic</a> .
Stateless UDP	For the settings required to configure the Stateless UDP traffic objective, refer to <a href="#">Stateless UDP Traffic</a> .

Parameter	Description
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">Data Traffic</a> .
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">Voice Traffic</a> .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">Ott Traffic</a> .
DNS Client	For the settings required to configure the DNS Client objective, refer to <a href="#">DNS Client Traffic</a> .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to <a href="#">Predefined Applications Traffic</a> .
Synthetic	For the settings required to configure the Synthetic objective, refer to <a href="#">Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG objective, refer to <a href="#">UDG Traffic</a> .
REST API Client	For the settings required to configure the REST API Client objective, refer to <a href="#">REST API Client</a> .

## Attacks

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

The following table describes the Attacks parameters.

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

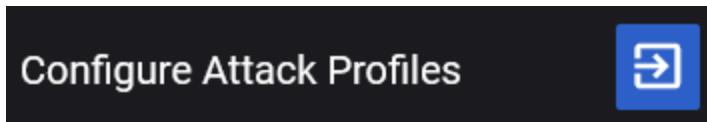
Parameter	Description
Configure Attack Profiles	Press the button to open the <a href="#">Attacks</a> settings page.

## Attack Profiles

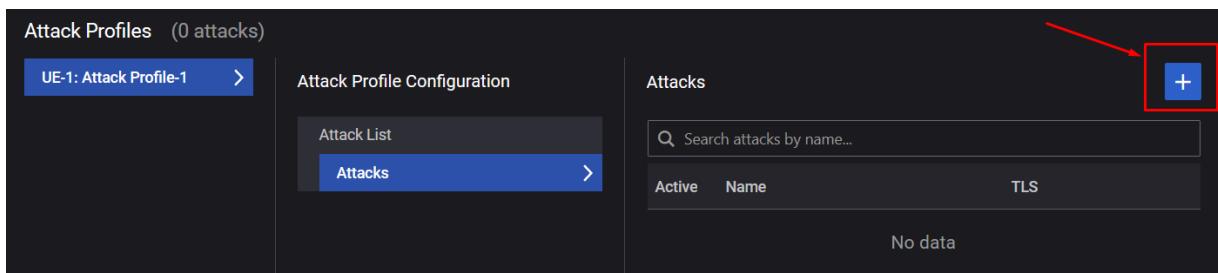
**IMPORTANT** Before this section to work properly, make sure you have installed the latest ATI security updates.

You can add more attack profiles as follows:

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



2. The Attack Profiles panel opens. Select the existent attack profile to open the **Attack Profile Configuration** panel.
3. A list with all profile attacks is displayed. Click on an the **Attacks** to open the configurator, then select the **Add** button.



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

### Adding attacks from the Library

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

Panel	Description
Filter attack(s)	You can filter the attacks by category name or value.
Attacks category panel	Each category listed includes more sub-categories and the number of existing attacks per each. Select a category/sub-category check-box to see the attacks included in the main panel
Select attack(s) from the table panel	The middle panel will be populated with the results of your filtered search. More actions include: <ul style="list-style-type: none"> <li>• further filter the attacks to add the one you need.</li> <li>• expand each attack to see a complete description and details about it.</li> <li>• press the Add icon (+) at the end of the row to select the attack to your profile.</li> </ul>
Summary of added attack(s) panel	You can view and manage the list of selected attacks. Press the Delete icon (trash bin) if you want to remove any of the attacks.
Add button	Once you have finished the selection, press this button to complete your action. The attacks will be added to your profile.

**Add Attack(s)**

[ATTACK LIBRARY](#) [CUSTOMIZE ATTACK](#)

**Filter attack(s)**

Filter by category name or value  Q

- [in\\_the\\_wild \(64\)](#)
- [public\\_poc \(65\)](#)
- [public\\_details \(29\)](#)
- [public\\_poc \(209\)](#)

▼  **Other**

- [.avi \(1\)](#)
- [.ppt \(1\)](#)
- [0-day \(3\)](#)
- [0day \(4\)](#)
- [1Day \(1\)](#)
- [ActiveX \(3\)](#)
- [Apache Struts \(1\)](#)
- [BO \(2\)](#)

>  [OWASP Top 10](#)

>  [Result](#)

>  [Target](#)

>  [Type](#)

>  [Vector](#)

[Reset filters \(463\)](#)

**Select attack(s) from table**

Filter attacks by name, description Q

Filter mode: AND ▼

50 attacks on this page

Name	Severity	Strikes	Direction	+
Firefox Browser Attacks	5 critical, 25 high...	43	s2c	<span style="color: #ccc;">+</span>
Generic Attacks Batch1	14 critical, 101 hi...	131	mixed	<span style="color: #ccc;">+</span>
Insecure Deserialization Attacks	6 critical, 7 high	13	c2s	<span style="color: #ccc;">+</span>

**Description:**  
Deserialization is the process of taking data structured for a format and rebuilding it into an object. The features of the native deserialization mechanism can be repurposed for malicious effect when operating on untrusted data. Attacks against deserializers have been found to allow denial-of-service, access control, and remote code execution attacks. This pre canned attack contains a collection of Insecure Deserialization attacks. It will run through each of the strikes one-by-one in order to test how well your implemented security controls protect your assets against these attacks. If these strikes are not blocked, they could compromise your application and/or put your customers and data at risk.

**Direction:**  
c2s

**Severity:**  
6 critical, 7 high

**Keywords:**  
Other: netsecopen\_fp\_avail, no\_no\_net, verified, netsecopen\_public, cisa\_vuln, one\_arm  
Result: remote\_code\_execution, Remote Code Execution  
Target: web\_application, web\_server  
Likelihood: private\_poc, public\_details, public\_poc, in\_the\_wild

64 attacks < 1 2 >

**Summary of added attacks (5)**

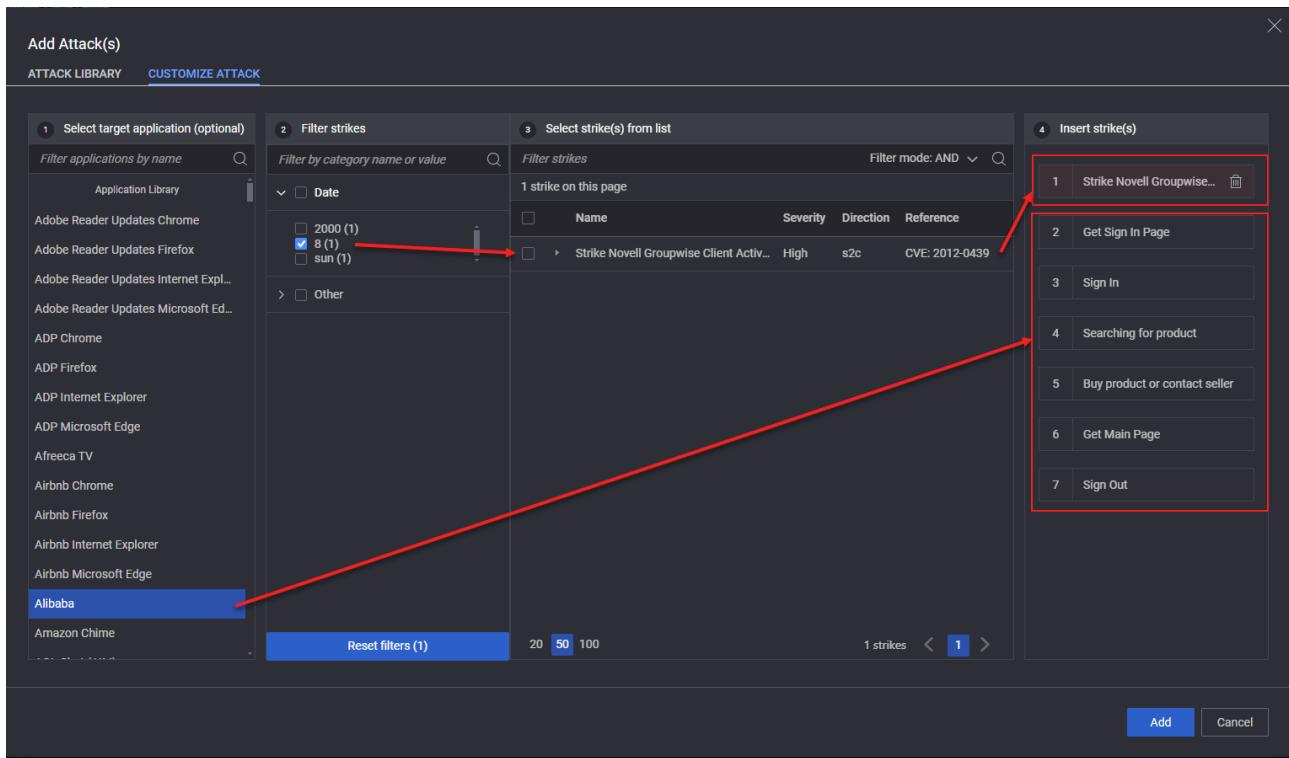
All Encrypted Attacks	<span style="color: #ccc;">trash bin</span>
Chrome Browser Attacks	<span style="color: #ccc;">trash bin</span>
Critical Strikes	<span style="color: #ccc;">trash bin</span>
Auth Bypass Attacks	<span style="color: #ccc;">trash bin</span>
LFI Attacks	<span style="color: #ccc;">trash bin</span>

Add Cancel

## Adding customized attacks

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

Panel	Description
Select target application (optional) panel	<p>Filter by the targeted application name to narrow down the results.</p> <div style="background-color: #2e6b2e; color: white; padding: 2px 10px; display: inline-block;"> <b>TIP</b> </div> <p>If you use this filter, it will automatically add specific strikes to the Insert Strike(s) panel.</p>
Filter strikes panel	<p>You can filter the attacks by category name or value.</p> <p>Each category listed includes more sub-categories and the number of existing attacks per each.</p> <p>Select a category/sub-category check-box to see the attacks included in the main panel</p>
Select strike(s) from the list	<p>This panel will be populated with the results of your filtered search (second panel search). More actions include:</p> <ul style="list-style-type: none"> <li>• further filter the strikes to add the one you need.</li> <li>• expand each attack to see a complete description and details about it.</li> <li>• select the attacks you need</li> </ul>
Insert strike(s) panel	<p>Depending on which of the previous options you have used, inserting strikes can be done in two ways:</p> <ul style="list-style-type: none"> <li>• press the Add button (+) in the empty list to add the selected strikes (this is applicable when selecting from the category list in the second panel)</li> <li>• select an Add button under/above an application strike that is already added in the list to mark the place and the order of execution for the selected category strike.</li> </ul> <div style="background-color: #2e6b2e; color: white; padding: 2px 10px; display: inline-block;"> <b>TIP</b> </div> <p>The category strikes will appear in the list with a dark red hallow.</p>
Add button	Once you have finished the selection, press this button to complete your action. The attacks will be added to your profile.



## Editing attacks

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

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

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

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

Parameter	Description
<i>Attack Settings</i>	
Destination Hostname	Destination hostname of the server.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
<i>Attacks Strikes and Actions</i>	
Strikes and Actions	
 Edit	Edits the strikes in the list. This will enable selecting and removing the strikes from the list.
 +	Add strikes and Actions button. This will open the <b>Add strikes and Actions</b> configuration dialog, where you can select and add more attacks to the selected attack, or assign actions.
	Connect strikes to server endpoint. This will open the <b>Misc Browser Attacks - Connect Strikes to Server Endpoints</b> page, where you can select and link the strikes that need to connect to a server.
Strikes and actions list	When selecting a strike from this list, you can: <ul style="list-style-type: none"> <li>remove the strike from the list</li> <li>drag up or down to change the item order</li> <li>configure specific properties for the selected strike, in the <b>Properties</b> panel. Refer to <a href="#">Application Actions</a> appendix for further details.</li> </ul>

## 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 <b>Stateless UDP</b> .
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 <b>uplink</b> and can not be modified since on the UE you can only

Parameter	Description
	configure the uplink flow.
Packet Rate	The rate at which the test generates uplink packets, measured in packets per second (pps).
Distributed Over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Delay(s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
Destination IP Address	The destination IP address to place in the IP packet.
Destination 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.
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 <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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 <b>Data</b> .
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 <b>Throughput</b> . The other options are: <b>Concurrent Connections</b> and <b>Connections Rate</b> .
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connections Rate per Second	Set the value for connections rate per second. This parameter is available only when Objective type is set to <b>Connections Rate</b> .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.  The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .

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

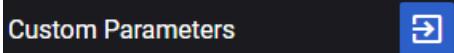
Parameter	Description
	Click the <b>Delete Flow</b> button to remove the flow from your configuration.
Transport Protocol available for Data	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> <li>If <a href="#">Optimize Throughput (per UE)</a> option is enabled: <b>TCP</b>, <b>TLS</b>, <b>QUIC</b> or <b>UDP</b>.</li> <li>If <a href="#">Optimize Throughput (per UE)</a> option is disabled: <b>TCP</b>, <b>TLS</b> or <b>UDP</b>.</li> </ul>
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get</b>, <b>HTTP Put</b>, <b>HTTP Post</b> and <b>FTP</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get</b>, <b>HTTPS Put</b> and <b>HTTPS Post</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Get</b>, <b>HTTP3 Put</b> and <b>HTTP3 Post</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional</b> (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)</li> </ul> <p><b>NOTE</b> UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receives the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds.</p>
Port	The port used by the flow.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.  Iterations number is set for each UE in the range, for example: if there is a range of 1000 UEs , and it has an objective of HTTP GET with 100 iterations, each of those UEs will get 100 HTTP pages.
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.

Parameter	Description
	<p><b>NOTE</b> Setting the page size on UE side will only influence PUT objectives, like HTTP PUT, HTTPs PUT and FTP PUT. To set the page size for GET objectives, the change must be operated on DN side.</p>
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
URL	The URL that is being accessed by the flow's protocol.
Destination Hostname	Destination hostname of the server. If DNS hostname resolution is enabled for the flow and Name Servers are configured under Global Settings, this name will be resolved before being used as L7 destination IP for the flow and included in HTTP headers. If empty, the "Address" from the previous fly-out level will be used as L7 destination IP for the flow.
Max Transactions per Connection	Set the value for this parameter.
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 ( <a href="#">DNNs Config</a> ).
QoS FlowID	Select a QoS Flow ID for this flow.

## Custom Parameters

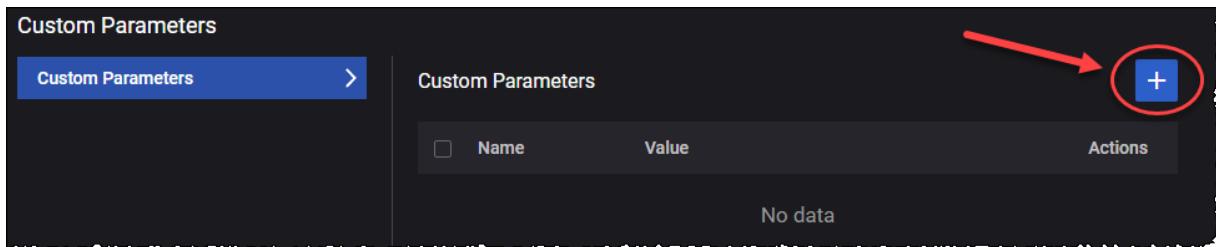
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

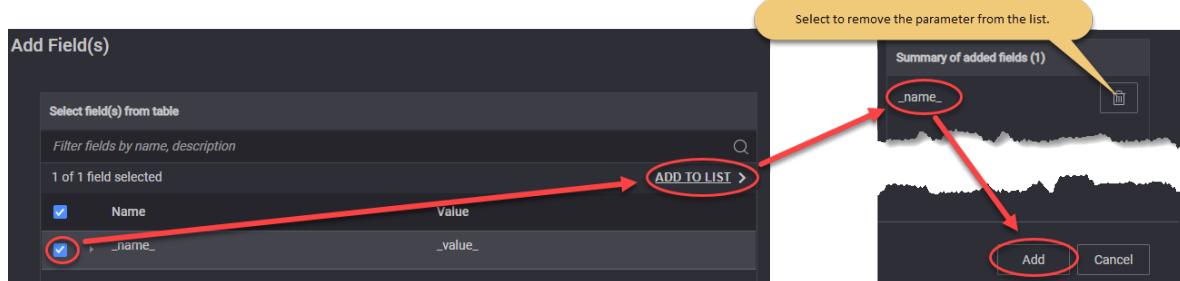
2. Select the **Add** button.



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 ...**



## 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 <b>Voice</b> .
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 <b>Simulated Users</b> 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: <b>IPv4</b> or <b>IPv6</b> .
Call Type	<p>Select the type of call from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>Basic Call</b></li> <li>• <b>Basic Call Mo</b> (Mobile Originated)</li> <li>• <b>Basic Call Mt</b> (Mobile Terminated)</li> <li>• <b>Custom Flow</b></li> </ul> <p>When creating a new test or when adding a new UE range, the Call Type default option is the <b>Basic Call</b>, which allows you to run a basic SIP call without the IMS entity and with DN simulating the Mobile Terminating (MT)</p>

Parameter	Description
	<p>side.</p> <p>When selecting <b>Basic Call MO/Basic Call MT</b>, the app will use a predefined SIP Flow intended for the use-case in which a DUT IMS or simulated IMS is involved.</p> <p>If the test requirements need an extended set of SIP flows or higher level of flexibility, it is recommended to use the <b>Custom Flow</b> Call Type, which enables the Flow Editor.</p>
<i>Flow Editor:</i>	<p><b>IMPORTANT</b> <i>This configurator becomes available only if Call Type is set to Custom Flow.</i></p> <p><i>Click to open the page and create a particular state machine for SIP calls that allows you a higher flexibility to customize the SIP message sequence and SIP headers/SDP body as desired. For settings, refer to <a href="#">Flow Editor</a> section.</i></p>
<i>Dial Plan:</i>	<i>For the settings required to configure the dial plan, refer to <a href="#">Dial Plan</a>.</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"> <li>• <b>TCP</b> - Transmission Control Protocol</li> <li>• <b>TLS</b> - Transport Layer Security</li> <li>• <b>UDP</b> - User Datagram Protocol</li> </ul>
Domain	Provide the domain name.
Persistent TCP Connection	If enabled, it will not close the TCP connection on the iteration end.
Enable IPSEC	Select this option to enable IPSEC.
Registration Refresh Time	Select whether to use a <b>Negotiated</b> refresh time, or a <b>Custom</b> type: <ul style="list-style-type: none"> <li>• <b>Negotiated</b> - the registration refresh will be sent after 50% of the expiration time received in <b>200 OK</b> response.</li> <li>• <b>Custom</b> - allows you to set the registration refresh interval</li> </ul>
Custom Registration Refresh Interval (s)	<p>This parameter appears only if <b>Registration Refresh Time</b> is set to <b>Custom</b>.</p> <p>The time interval (in seconds) to send SIP Registration Refresh.</p>
Number of Loops after Registration to Send Deregistration	This parameter will send the SIP Deregister at the end of each configured iteration number.

Parameter	Description
Advanced SIP Settings	For more details about these settings, refer to <a href="#">Advanced SIP Settings</a> .
<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 Real-Time Transport Control Protocol (RTCP).
Enable SRTP	Select this option in order to enable Secure Real-time Transport Protocol (SRTP).
RTP Session Duration (ms)	Set the value for the session duration.
<i>Audio settings:</i>	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
<i>Video Settings:</i>	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
<i>MSRP Settings:</i>	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
<i>MCTTP Settings</i>	<i>For the configuration of MCTTP settings, refer to <a href="#">MCPTT Settings</a>.</i>
<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"> <li>• <b>None</b></li> <li>• <b>EVS/AMR IPv4</b></li> <li>• <b>NB Codecs IPv6</b></li> <li>• <b>AMR-WB IPv6</b></li> <li>• <b>Multimedia IPv4</b></li> </ul>
<i>QoE Settings</i>	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

## Flow Editor

Press  to open the editor's window. The following settings are available:

Parameter	Description
Procedures Library	<p><b>TIP</b> This library can also be accessed from Test Overview &gt; Procedures Library, while the procedures are managed from the <a href="#">Settings &gt; Resource Library</a>.</p> <p>Select to access the Procedures Library, where you will find the following categories:</p> <ul style="list-style-type: none"> <li>• <b>SIP</b> - will include the procedures related to SIP signaling.</li> <li>• <b>Media</b> - will include the procedures related to media (audio or/and video)</li> <li>• <b>Flow</b> - will include the Start and Stop procedures used to define an iteration. The number of iterations can be configured per each UE range on the Voice objective, Dial Plan section (0 meaning infinite loops).</li> </ul> <p>See <a href="#">Procedures Library</a> for more information.</p>
Current Range	This field will be automatically populated with the name of the UE range on which the Voice application traffic is configured.
Add required procedures first > Procedures	Add the procedures required for this custom flow.
Linked Range	Select from the drop-down the UE range that will be connected. Then, add the procedures corresponding to the configuration of state machine.

Note that every procedure added under the Procedures list includes an **Add +** button and an **Expand** button:

- Use the Expand button to see the **Next On Success** and **Next on Error** configuration fields for the respective procedure. Proceed on setting up these fields for each procedure added.
- Use the **Add** button to add more steps to the procedure. Set the procedures as above.
- The red connections that appear between procedures will let you know how these are connected.

See also the [Procedures Resources \(SIP/Media/Flow\)](#) section for complete information on:

- [procedures resources and their management](#)
- [adding predefined procedures](#) from the Resource Library
- [using the Flow Editor](#) and other configurations required
- [creating a procedure from scratch](#)

## Dial Plan

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

Parameter	Description
DNN	Select the DNN from the drop-down list.
Destination IP	The destination IP address.
Destination IP Increment	The value by which the destination IP is incremented.
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
MCC	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	<p>The MSIN value that will be assigned to the first simulated UE in the range.</p> <p><b>About MSIN ...</b></p> <p>The Mobile Subscriber Identification Number (MSIN) is a number that a wireless operator uses to uniquely identify a mobile phone. It is—at most—10-digits long. The MSIN is used (in combination with the MCC and MNC) to form the International Mobile Subscriber Identity (IMSI) number.</p>
IMSI Phone Increment	The value by which the IMSI phone number is incremented.
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.
Source Phone Increment	The value by which the destination phone number is incremented.
Destination Port	The destination port number.

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Voice	Select the QoS flow used for voice from the drop-down list.

Parameter	Description
<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"> <li>• <a href="#"><b>AMR</b></a> - 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.</li> <li>• <a href="#"><b>AMR-WB</b></a> - 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.</li> <li>• <a href="#"><b>EVS</b></a> - 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.</li> <li>• <a href="#"><b>PCMU</b></a></li> <li>• <a href="#"><b>PCMA</b></a></li> <li>• <a href="#"><b>iLBC</b></a></li> <li>• <a href="#"><b>G722</b></a></li> <li>• <a href="#"><b>G723</b></a></li> <li>• <a href="#"><b>G729</b></a></li> </ul> <p>The parameters of each audio codec are presented below.</p>

## AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth efficient:</b> In the bandwidth efficient format only the full</li> </ul>

Parameter	Description
	<p>payload is octet aligned, so fewer padding bits are added.</p> <ul style="list-style-type: none"> <li>• <b>Octet aligned:</b> 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.</li> </ul>
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"> <li>• <b>Full header</b> - 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.</li> <li>• <b>Compact</b> - 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.</li> </ul>
Bitrate	Indicates the mode(bitrate) of the EVS codec. Select the value from the drop-down list.

## PCMU/PCMA/iLBC/G722/G723/G729

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

## Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Video	Select the QoS Flows ID(s) from the drop-down list.
<i>Video Codecs</i>	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

## MSRP Settings

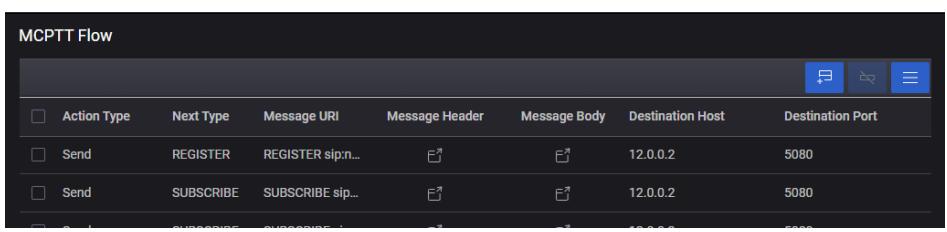
The parameters required for MSRP settings are presented in the table below.

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

## MCPTT Settings

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

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

Parameter	Description																					
MCPTT Message Format	The MCPTT message format defined according to TS 24.380 standard.																					
MCPTT Group	The first MCPTT Group ID.																					
MCPTT Group Size	The number of participants per MCPTT group call.																					
Use CRLF in flow csv	If enabled, it will use the CRLF line terminator in the generated CSV of the configured MCPTT flow. If disabled, it will use LF.																					
MCPTT Flow 	Press the <b>Open MCPTT Flow Editor</b> button to open the configuration page. Use the <b>Add New Row</b> button, and then select each column field to edit the flow.  <table border="1"> <thead> <tr> <th>Action Type</th> <th>Next Type</th> <th>Message URI</th> <th>Message Header</th> <th>Message Body</th> <th>Destination Host</th> <th>Destination Port</th> </tr> </thead> <tbody> <tr> <td>Send</td> <td>REGISTER</td> <td>REGISTER sip:n...</td> <td></td> <td></td> <td>12.0.0.2</td> <td>5080</td> </tr> <tr> <td>Send</td> <td>SUBSCRIBE</td> <td>SUBSCRIBE sip...</td> <td></td> <td></td> <td>12.0.0.2</td> <td>5080</td> </tr> </tbody> </table>	Action Type	Next Type	Message URI	Message Header	Message Body	Destination Host	Destination Port	Send	REGISTER	REGISTER sip:n...			12.0.0.2	5080	Send	SUBSCRIBE	SUBSCRIBE sip...			12.0.0.2	5080
Action Type	Next Type	Message URI	Message Header	Message Body	Destination Host	Destination Port																
Send	REGISTER	REGISTER sip:n...			12.0.0.2	5080																
Send	SUBSCRIBE	SUBSCRIBE sip...			12.0.0.2	5080																

## 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.

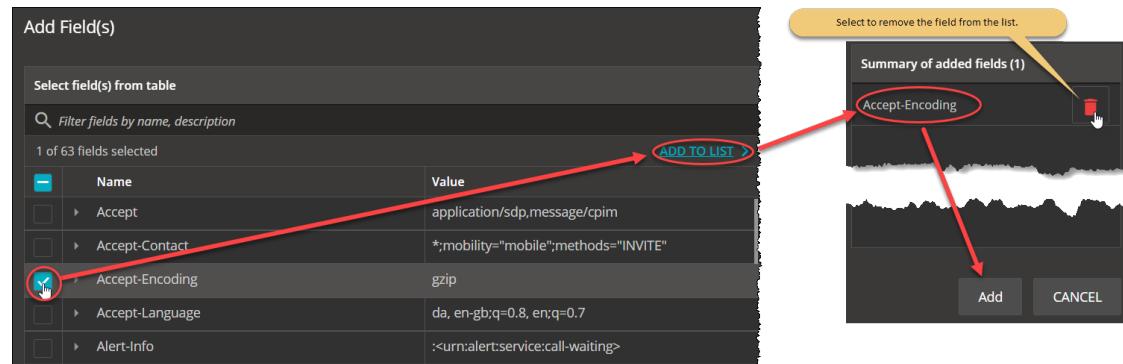
**NOTE**

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, IETF RFC 3310	nextnonce="47364c23432d2e131a5fb210812c"

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
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 3261	3600
Feature-Caps	IETF RFC	+3gpp.trf=sip:trf3.operator3.com

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
	6809, 3GPP TS 24.229	
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC 4028	60
Organization	IETF RFC 3261	Keysight
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC 3327	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>
P-Called-Party-ID	IETF RFC	sip:user1-business@example.com

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
	7315	
P-Chargin g-Function-Addresse s	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Chargin g-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
Permissi on-Missing	IETF RFC 5360	userC@example.com
P-Preferre d-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferre d-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenti cate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=False,algorithm=MD5
Proxy-Authoriz ation	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-	IETF	Visited network number 1

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
Visited-Network-ID	RFC 7315	
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

Parameter	Description	Value
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

## SIP Authentication

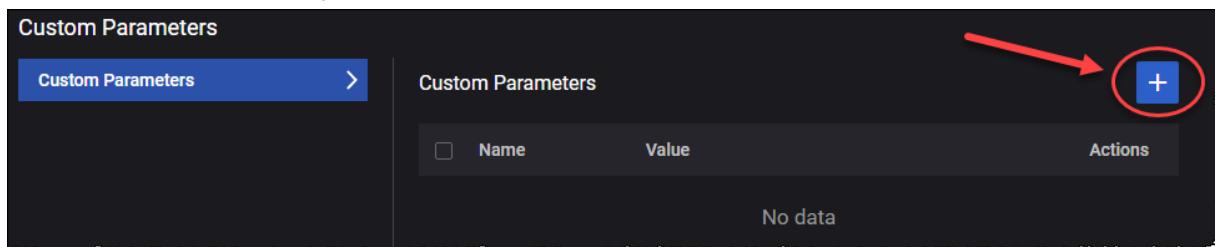
The parameters required for SIP authentication are presented in the table below.

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

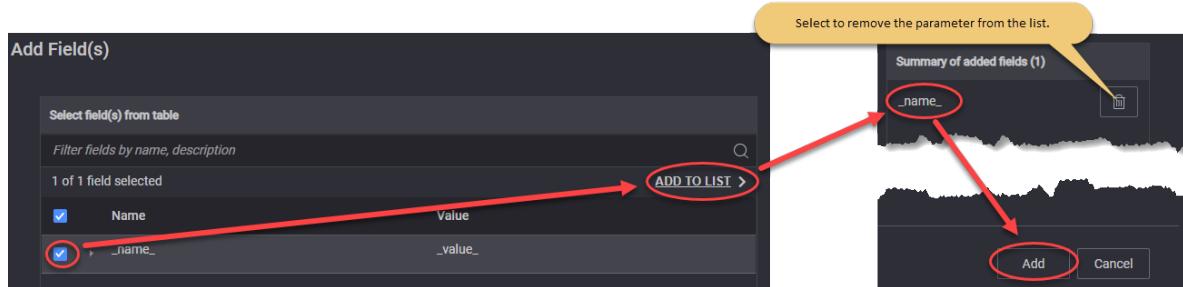
1. The Custom Parameters panel, select the **Add** button.



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
timeoutSIP	Global timeout in milliseconds for any SIP message. Default is set to standard	32000

Parameter	Description	Value
	32000ms. Use this parameter to modify the default value.	
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"> <li>• <b>hmac-sha-1-96</b></li> <li>• <b>aes-gmac</b></li> <li>• <b>null</b></li> </ul>
Encryption Algorithm	Select the encryption algorithm: <ul style="list-style-type: none"> <li>• <b>aes-gcm</b></li> <li>• <b>aes-cbc</b></li> <li>• <b>null</b></li> </ul>

### 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 <b>Video OTT</b> .
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: <b>Simulated Users</b> or <b>Throughput</b> .
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.

Parameter	Description
	The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .
Advanced OTT	Select the <b>Open Advanced OTT</b> button to enable and configure <a href="#">Advanced OTT Settings</a> .

## 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"> <li>To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul>
<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"> <li><b>DASH</b></li> <li><b>HLS</b></li> </ul>
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
URL	Select the URL from the drop-down list populated with the defined on the server.
Play Until End	If this check box is selected, the Play Duration field is disabled and the original playtime is used.

Parameter	Description
Play Duration (sec)	This field is available only if the Play Until End check box is not selected. It allows you to set a custom playtime.
Transport	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Quality Control</a> pane.
Advanced Client settings	These settings are presented in the <a href="#">Advanced Client Settings</a> 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: <b>Disabled</b> or <b>Mode 0</b> .
.Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Adaptive Bit Rate</b></li> <li>• <b>Quality Predefined Levels</b></li> <li>• <b>Lowest Quality</b></li> <li>• <b>Highest Quality</b></li> </ul>
Number of segments	This field is available and editable only when the Quality Control Mode is set to <b>Adaptive Bit Rate</b> .
<i>Play Profiles:</i> The following settings are available and editable only when the Quality Control Mode is set to <b>Quality Predefined Levels</b> .	

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"> <li>• <b>Stay at Current Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lower Bitrate</b></li> <li>• <b>Change to the Higher Bitrate</b></li> </ul>
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to <b>Change to Higher Bitrate</b> or <b>Change to Lower Bitrate</b> .
Play Until End	If this check box is selected, the <b>Play duration</b> field is disabled and the original playtime is used.
Play duration(sec)	This field is available only if the <b>Play Until End</b> check box is not selected. It allows you to set a custom playtime.

## Advanced Client Settings

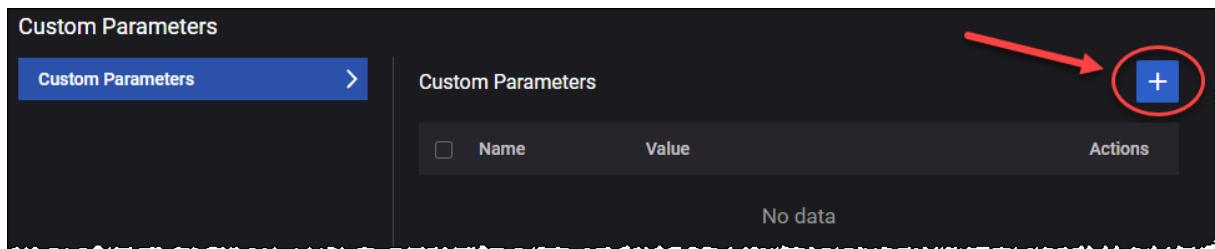
The parameters required for Advanced Client settings are presented in the table below.

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 <a href="#">Custom parameters</a> .

## Custom Parameters

You can add custom parameters as follows:

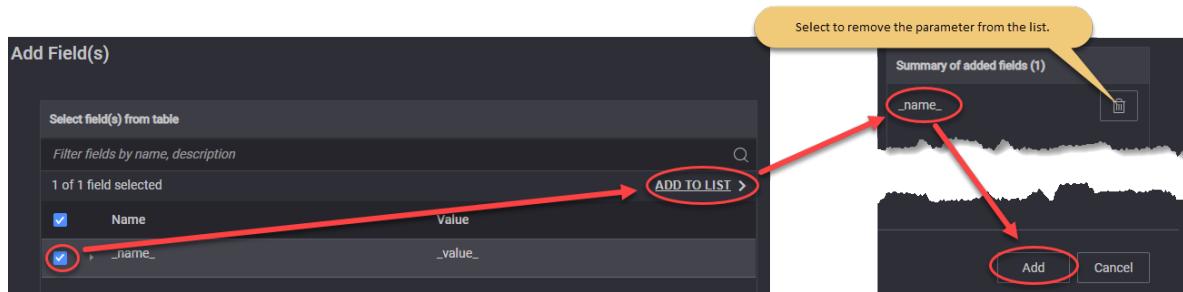
1. Select the **Open Custom Parameters** tile. The Custom Parameters panel opens.
2. Select the **Add** button.



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 <b>DNS Client</b> .
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 <b>Simulated Users</b> 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>

<b>Parameter</b>	<b>Description</b>
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: <b>IPv4</b> or <b>IPv6</b> .
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"> <li>• To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>• To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul> <p>Refer to <a href="#">Flow</a> for a description of the configuration settings for these traffic flows. Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Flow</b> button to remove the flow from your configuration.
Type	By default, the type is set to <b>DNS Client</b> .
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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
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 ( <a href="#">DNNs Config</a> ).
QoS FlowID	Select a QoS Flow ID for this flow.

## Custom Parameters

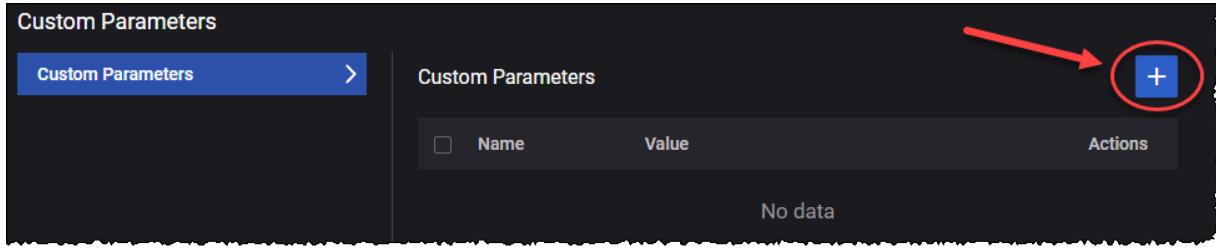
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

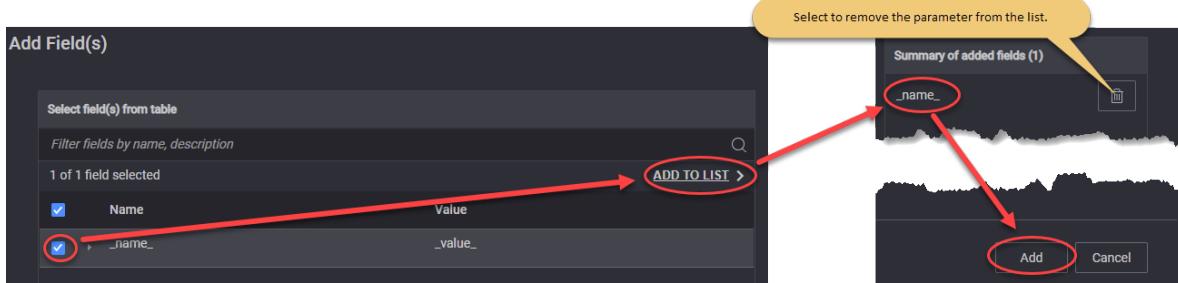
2. Select the **Add** button.



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 <b>ICMP Client</b> .
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 <b>Simulated Users</b> 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: <b>IPv4</b> or <b>IPv6</b> .
Traffic Flow	Refer to <a href="#">Traffic Flow</a> 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 ( <a href="#">DNNs Config</a> ).

## 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 <b>Data</b> .
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 <b>Simulated Users</b> 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 ( <a href="#">DNNs Config</a> ).
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: <b>IPv4</b> or <b>IPv6</b> .

## 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 <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b> (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (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 <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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: <b>Initiator</b> and <b>Responder</b> . Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .

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

## Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>Synthetic</b> .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).</p>
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of

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

The following table describes the Traffic Flow parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Client Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
Server Burst Interval	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
Server Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

## UDG

The following table describes the UDG parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>UDG</b> .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
Delay application	The time (in milliseconds) to wait before the application traffic flows start

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

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

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

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>UDP</b> .
Out of Band Signaling	<p>Select this check-box to enable OOB signaling. More details about the required parameters <a href="#">here</a>.</p> <p><b>IMPORTANT</b> To use the OOB feature, the OOB interface must be set in Agent Management window.</p>
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Source Port	The local port for client data connection.
Reconnect Timeout (ms)	The time interval after which the client attempts to reconnect after the connection was interrupted. 0 means that reconnect is disabled.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
UDG Traffic Parameters	Select to enable and configure the <a href="#">UDG Traffic Parameters</a> .
Transaction	Select to enable and configure the <a href="#">Transaction</a> parameters.

Parameter	Description
Status Query Interval	Timeout for keepalive packets on server. The server will wait for the <code>keepAliveInterval</code> value multiplied by <code>keepAliveExpiryCount</code> value.
Keepalive Interval	The time interval, in milliseconds, between UDG statistics requests (RESULT). A zero value means this feature is disabled.
Keepalive Expiry Count	The time to wait for UUDG to reconnect. A 0 value means the reconnect is disabled (in milliseconds).

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

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

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

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

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

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

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

## REST API Client

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

The following table describes the REST API Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>REST API Client</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	This field is set to <b>Simulated Users</b> and cannot be modified.
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>TLS</b>
REST API Flow	The name of list of REST API Client sequential operations and transitions emulated by each REST API Client.  The REST API Flow is initially loaded into LoadCore's Resource Library, and then added to the test as a <a href="#">Global Playlists</a> . The list is defined in CSV format, following specific rules. Refer to <a href="#">Work with the Resource Library on page 73</a> section for further information.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before starting the Attacks objective traffic.
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .
Iterations	If is set to <b>0</b> , it will be iterated on continuous loop during sustain time. If set to <b>1</b> , it will be executed only one time.  <b>IMPORTANT</b> Values greater than 1 are not allowed.
Max Transactions per Connection	The maximum amount of transactions an application can make on one connection.

Parameter	Description
Enable DNS Query per Connection	If enabled, will process only one DNS query per TCP connection.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.  The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Selective Acknowledgments	Select the toggle button to enable this option.

Parameter	Description
<i>TLS Settings</i>	See <a href="#">TLS Settings</a> table for more details.
<i>Custom Parameters</i>	For more details, refer to <a href="#">Custom parameters</a> .

## TLS Settings

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

## Custom Parameters

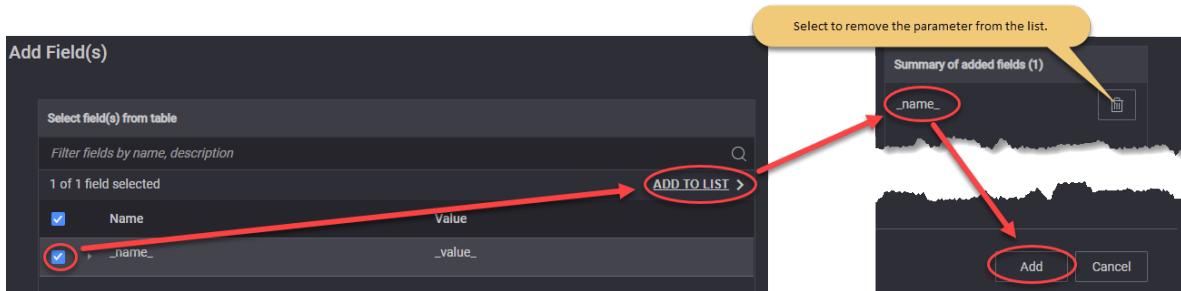
From this section you can add custom parameters fields:

- **Custom Parameters**

You can add custom parameters as follows:

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

**For example ...**



## How to Configure the REST API Client

1. Define your REST API flow in an CSV file, following the rules described in the [REST Client Flow specifications](#).
2. Load the CSV as a Global Playlist in LoadCore user interface:
  - a. Go to **Global Settings > Global Playlist**.
  - b. Add a new Playlist using the **+** button.
  - c. **Name** the new Playlist - it will be used in the REST API Client application configuration.
  - d. **Upload** the CSV created at **Step 1**.
3. In the User Plane UE section, select the **REST API Client** application traffic.
4. Set all necessary parameters on required by the application (see [REST API parameters table](#) above):
  - on **Transport protocol** select **TCP** or **TLS** (version 1.2 and 1.3 configurable from TLS Settings).
  - the **Objective type** is automatically set to **Simulated users**.
  - add the **REST API Flow** name that defines the REST sequence of actions defined in the Global Playlist.
  - set the **Max Transactions per Connection**- for REST API Client application, one "Transaction" points to all REST actions (HTTP requests) specified in REST flow.
  - Set all other common parameters.

## REST Client Flow specifications

The REST Client flow will be specified in CSV format state-by-state. For each State in flow, three main commands must be specified, and one special command at the end of list:

Command	Condition	Description
<b>Action</b>	Mandatory	<p>Indicates what actions should be executed in the current State and what transitions can be executed. The following rules are in place:</p> <ul style="list-style-type: none"> <li>• up to 4 transitions are allowed. Maximum 4 pairs of (Conditions, NextState) are used from CSV.</li> <li>• Method, Headers and Body should be specified in separate columns.</li> <li>• Method, Headers and Body can contain dynamic parts specified by flow user variables.</li> </ul>
<b>Extract</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>Specifies if some elements from the last HTTP response should be extracted in user variables for further utilization in flow:</p> <ul style="list-style-type: none"> <li>• extractions are specified using (backqoute_separated_path, userVar) pairs.</li> <li>• up to 3 extractions per REST(HTTP) response are allowed.</li> </ul>
<b>Statistics</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>User-defined Counters can be incremented when the condition is fulfilled. The configuration is done in pairs of (condition, UserCounter).</p>
<b>ENDMARKER</b>	Mandatory	This special command is mandatory to indicate the end of REST API flow. No other command will be executed after the ENDMARKER was executed. It can be inserted anywhere in the Playlist, on the first column.

## REST user flow variables

There are 10 flow variables with predefined names (userVar1, userVar2,...,userVar10) available for store extracted values from REST Commands during flow duration. On each REST Command, you can configure what to extract from the received Response, and in what variable.

Each variable can be overwritten at anytime, therefore a variable can be persistent during the flow duration, or only temporary, until overwrite.

## Predefined Applications Traffic

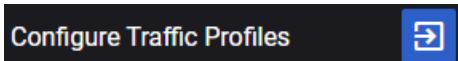
The following table describes the Predefined Flows Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Predefined Applications</b> .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Simulated Users</b></li> <li>• <b>Throughput</b></li> <li>• <b>Connections Per Second</b></li> </ul>
Throughput (kbps)	<p><b>IMPORTANT</b> This parameter is available only when <a href="#">Objective Type</a> is set to <b>Throughput</b>.</p> <p>The desired throughput (in kbps) for the combined traffic flows that will be generated.</p>
Connections Per Seconds	<p><b>IMPORTANT</b> This parameter is available only when <a href="#">Objective Type</a> is set to <b>Connections Per Second</b>.</p> <p>Set the number of connections.</p>
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size 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.
Configure Traffic Profiles	<p>Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions.</p> <p>Refer to <a href="#">Traffic Profile</a> for a description of the configuration settings for these traffic profiles.</p>

## Traffic Profile

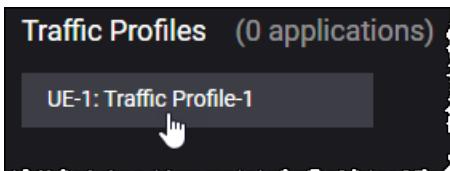
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

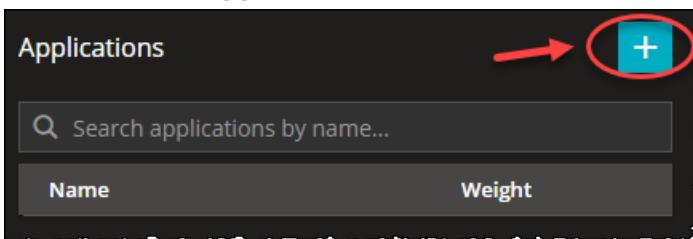
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

## Applications

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

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



The Add Application(s) window opens.

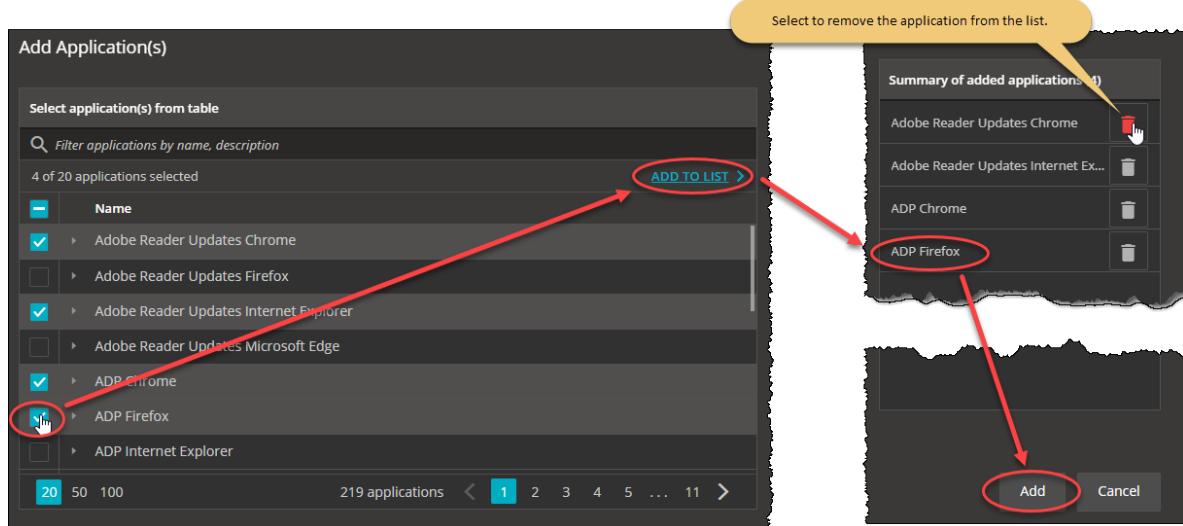
2. From the Add Application(s), select the applications you want to add and select **ADD TO LIST** to move them to the added applications section. To add the applications to your configuration select **Add**.

**NOTE**

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

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.

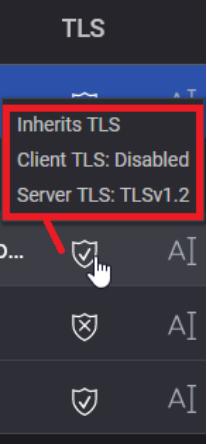
**For example ...**

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.
TLS	Hover over this icon to see the TLS status for this attack. You can quickly review the TLS settings behind this status.

Field	Description
	 <p>The screenshot shows a list of TLS settings. The first item, "Inherits TLS", is highlighted with a red box and has a checkmark icon next to it, indicating it is selected. Below it are two other items with shield icons and "AI" labels.</p>
	<p>For further details on this setting, see <a href="#">Application Advanced Settings &gt; TLS Settings</a>.</p>
Weight	<p>Set the application weight using the adjustment button. If the primary objective of a Traffic Profile is set to <b>Throughput</b>, the selected weight distribution time depends on the types and number of applications added to the application list.</p>
Action Buttons 	<ul style="list-style-type: none"> <li>• <b>Rename</b> - Select to rename the application.</li> <li>• <b>Advanced Settings</b> - for more information, refer to <a href="#">Advanced Settings</a>.</li> <li>• <b>Delete</b> - Select to delete the application.</li> </ul>

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

**For example ...**

The screenshot shows the LoadCore configuration interface. On the left, the 'Applications' section lists four predefined applications with their names and weights:

Name	Weight
Adobe Reader Updates Chrome 1	1
Adobe Reader Updates Firefox 2	1
Adobe Reader Updates Internet Exp...	1
Adobe Reader Updates Microsoft E...	1

On the right, the 'Application Settings' section contains fields for Destination Hostname, DNN ID, and QoS Flow ID. Below it, the 'Application Actions' section lists actions for each application, such as '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.

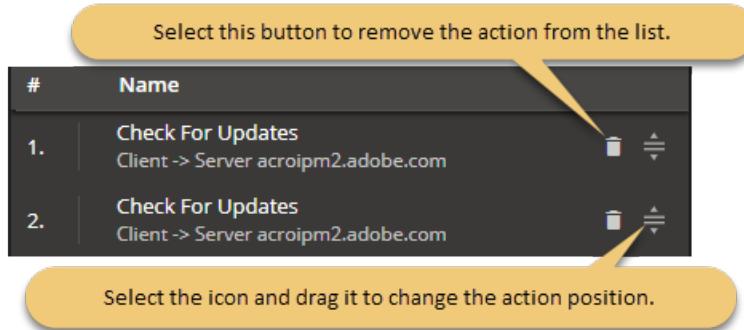
Field	Description
Destination Hostname	The application name.
DNN ID	Select the DNN from the drop-down list.
QoS Flow ID	Select a QoS Flow ID from the drop-down list.

## 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:

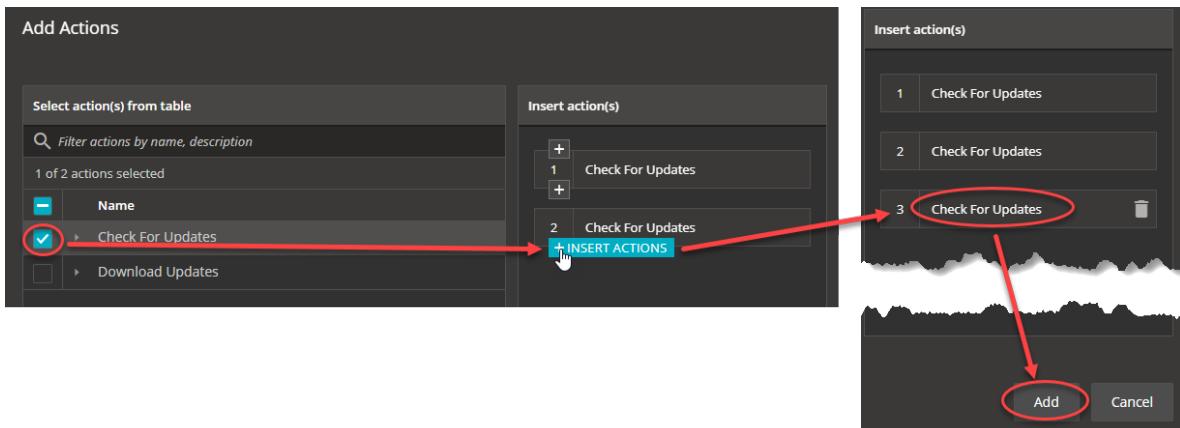
1. Use the icons available for each icon in order to remove it or to change its position in actions list.  
**For example ...**



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.

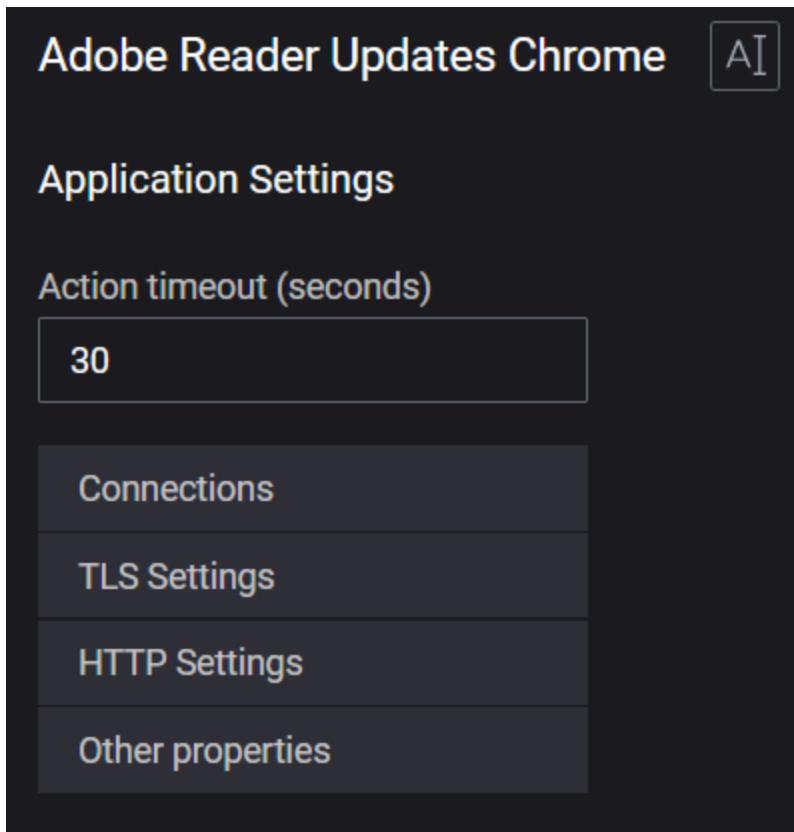
## Application Advanced Settings

**NOTE** This section is also applicable for Attacks Settings.

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

- **Action timeout** field - set the timeout, in seconds
- **Connections** section
- **TLS Settings**
- **HTTP Settings**
- **Other 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. Depending on your application/attack, you may encounter two options for this parameter: <ul style="list-style-type: none"> <li>• <b>User input</b></li> <li>• <b>Playlist file</b> - allows you to add a custom playlist, using the <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.</li> </ul>
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	Select the check box to enable it this option.

Field	Description
disabled	

Under the **TLS Settings** section, the application/attack TLS Settings fields are displayed, as follows:

Field	Description
Inherit TLS	<p>This option is enabled by default.</p> <ul style="list-style-type: none"> <li>When Inherit TLS is <b>enabled</b>, the client and server agent inherit the SSL profile configured under the TLS Settings tab on the Application Profile or Attack Profile page.</li> <li>When Inherit TLS is <b>disabled</b>, and the <b>Client TLS</b> is <b>enabled</b>, the client receives an SSL profile for each application or attack.</li> <li>When Inherit TLS is <b>disabled</b>, and the <b>Server TLS</b> is <b>enabled</b>, the server receives a single SSL profile.</li> </ul> <p><b>NOTE</b> The server TLS settings must be identical across all profiles for the same agent. If multiple server TLS profiles are configured at different levels for the same agent, an error is triggered informing you that there are differences between the profiles.</p>
Client TLS	<p><b>IMPORTANT</b> <i>This section appears only if the <b>Inherit TLS</b> parameter is disabled.</i></p> <p><i>Click this option to open the Client TLS Settings panel. Refer to <a href="#">TLS Settings</a> for further configuration of the parameters.</i></p>
Server TLS	<p><b>IMPORTANT</b> <i>This section appears only if the <b>Inherit TLS</b> parameter is disabled.</i></p> <p><i>Click this option to open the Server TLS Settings panel. Refer to <a href="#">TLS Settings</a> for further configuration of the parameters.</i></p>

Under the **HTTP Settings** section, the application/attack HTTP fields are displayed, as follows:

Field	Description
Inherit HTTP	<p>When Inherit HTTP is enabled, the client and server agent inherit the HTTP settings configured at the traffic profile level.</p> <p>This option is enabled by default, with the following exceptions:</p> <ul style="list-style-type: none"> <li>Configuration imported from older software versions, which had different values than the default ones in the HTTP profile for the parameters in the <b>Parameters</b> section under <b>Application advanced settings</b></li> <li>Applications that come from ATI with profiles that differ from the default predefined profiles. For example: Facebook Chrome which had the Inherit HTTP option enabled, or Facebook Mozilla which had the Inherit HTTP option disabled.</li> </ul> <p>Other limitations for 3.0 and newer versions:</p> <ul style="list-style-type: none"> <li>For the <b>HTTP App</b>, the headers defined at both the application level and traffic</li> </ul>

Field	Description
	profile level will be ignored when the <b>HTTP App</b> has <i>request</i> and <i>response</i> headers that are exposed as <b>Action</b> parameters, in which case those headers will be used. Overriding this behavior and using the HTTP profile headers instead is not currently supported.
Client HTTP	<p><b>IMPORTANT</b> <i>This section appears only if the <b>Inherit HTTP</b> parameter is disabled.</i></p> <p><i>Click this option to open the Client HTTP Settings panel. Refer to <a href="#">HTTP Settings</a> for further configuration of the parameters.</i></p>
Server TLS	<p><b>IMPORTANT</b> <i>This section appears only if the <b>Inherit HTTP</b> parameter is disabled.</i></p> <p><i>Click this option to open the Server HTTP Settings panel. Refer to <a href="#">HTTP Settings</a> for further configuration of the parameters.</i></p>

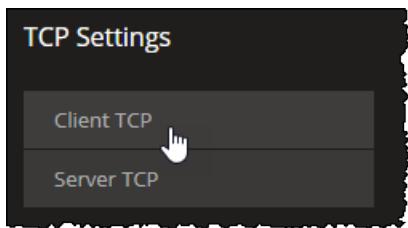
Under the **Other properties** section, the application/attack settings properties fields are displayed, as follows:

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"> <li>• Chrome</li> <li>• Firefox</li> <li>• Opera</li> <li>• Microsoft Edge</li> <li>• Internet Explorer</li> <li>• Safari</li> <li>• Android</li> </ul>
Action Timeout (seconds)	Set the action timeout in seconds.
Connection Persistence	Select an option for the connection persistence: <ul style="list-style-type: none"> <li>• <b>Standard</b> - inherits the behavior with respect to the HTTP version (1.0 or 1.1).</li> <li>• <b>Disabled</b> - enforces connection closing following every HTTP message.</li> <li>• <b>Enabled</b> - enforces connection persistence through explicit keep-</li> </ul>

Field	Description
	alive.
HTTP Version	Select the HTTP version used: <ul style="list-style-type: none"> <li>• <b>HTTP/1.0</b></li> <li>• <b>HTTP/1.1</b></li> </ul>
Receive retries	The number of times the receive will be retried.
Receive timeout	The receive timeout used for the UDP connection.

## TCP Settings

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



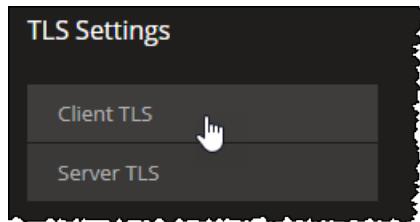
These parameters are configurable for both **Client** and **Server** settings, as presented in the following table.

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 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

Parameter	Description
	your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
RFC1323 TCP timestamps enabled	Enable or disable the stamp using the toggle button. If enabled, the client or server inserts an RFC 1323 timestamp into each packet. <p><b>NOTE</b> Enabling the TCP Timestamp option adds 12 bytes to the TCP header. This reduces the effective configured MSS.</p>
Selective acknowledgments	When enabled, the data receiver can inform the sender about all segments that have arrived successfully. Therefore, the sender will retransmit only the segments that have actually been lost. When disabled, the exchange of selective acknowledgments between the endpoints is no longer permitted. This is the default value. <p><b>IMPORTANT</b> Must be enabled for both client and server, to take effect. When running a mix of apps and attacks, attack profile's settings will be applied to both profiles, since it has the higher precedence.</p>

## TLS Settings

The following UI elements are available on the TLS Settings tab under the Traffic Profile/Attack 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
	Select this button to apply the client TLS settings configured at the currently selected application or attack level to the other existing application or attack profiles. When selecting this button, you are prompted to choose one or multiple client TLS profiles from the current configuration to which the current TLS settings will be applied.
Enable TLS traffic	<p><b>IMPORTANT</b> For Attacks traffic Profiles only.</p> <p>If enabled, the client will initiate all connections to the destination over TLS, based on the settings below. If disabled, connections will be established in plaintext.</p> <p>Even if Enable TLS traffic is not active, the client agent may use the TLS settings based on responses it receives from the server. For example, if the server sends an HTTP Redirect (3xx) response with a https:// URL, when the client agent follows that redirect, it will initiate a TLS connection based on the configured TLS settings.</p>
TLSv1.2	<p>Select the check box to enable it.</p> <p>The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Disable</li> <li>• Session ticket</li> <li>• Session ID</li> </ul> <p><b>IMPORTANT</b> Session reuse method is available only if TLSv1.2 is enabled.</p>
Session reuse count	<p>The number of simultaneous connections that can share the same Session ID or Session ticket.</p> <p><b>IMPORTANT</b> This option appears only if client TLSv1.2 is enabled, and the <b>Session reuse method</b> is set to either the <b>Session ticket</b> or the <b>Session ID method</b>.</p>
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).
Send close notify	If enabled, it will send a close notify message.
TLSv1.3	Select the check box to enable it.

Parameter	Description
<i>The following options became available:</i>	
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	This option is enabled by default. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).
Send close notify	If enabled, it will send a close notify message.

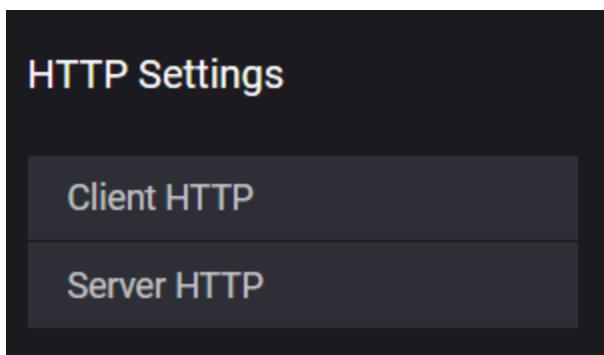
### Server TLS Settings

Parameter	Description
	Select this button to apply the client TLS settings configured at the currently selected application or attack level to the other existing application or attack profiles. When selecting this button, you are prompted to choose one or multiple client TLS profiles from the current configuration to which the current TLS settings will be applied.
<i>TLSv1.2</i>	<i>Select the check box to enable it.</i> <i>The following options became available:</i>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	Select the Session Reuse Method from the drop-down list: <ul style="list-style-type: none"> <li>• Disable</li> <li>• Session ticket</li> <li>• Session ID</li> </ul> <p><b>NOTE</b> Session reuse method is available only if TLSv1.2 is selected.</p>
Immediate close	If enabled, the endpoint closes the TCP connection immediately after sending the TLS CLOSE message (i.e., the endpoint does not wait for a confirmation from the other end).
Send close notify	If enabled, it will send a close notify message.
<i>TLSv1.3</i>	<i>Select the check box to enable it.</i> <i>The following options became available:</i>

Parameter	Description
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	Select the check box to enable it. It allows for compatibility with middleboxes which do not support TLSv1.3.
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.
<i>SNI Enabled</i>	<i>Select the toggle button to enable the server name indicator. If enabled, the following <b>SNI Settings</b> become available for each server name selected:</i>
Certificate file	Select <b>Upload</b> to add your certificate file or <b>Clear</b> to remove it.
Key file	Select <b>Upload</b> to add your key file or <b>Clear</b> to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select <b>Upload</b> to add your DH file or <b>Clear</b> to remove it.
<i>Certificate file</i>	<i>Select <b>Upload</b> to add your certificate file or <b>Clear</b> to remove it.</i>
<i>Key file</i>	<i>Select <b>Upload</b> to add your key file or <b>Clear</b> to remove it.</i>
<i>Key file password</i>	<i>Enter your key file password.</i>
<i>DH file Traffic</i>	<i>Select <b>Upload</b> to add your DH file or <b>Clear</b> to remove it.</i>

## HTTP Settings

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



**NOTE**

HTTP settings can be configured both at the traffic profile level for all the available applications or attacks, and at a per-application or per-attack level.

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

### **Client HTTP Settings**

Parameter	Description
<i>Client HTTP Settings</i>	
HTTP profile	Select the client HTTP profile from the available options: <ul style="list-style-type: none"> <li>• <b>Android</b></li> <li>• <b>Chrome</b></li> <li>• <b>Microsoft Edge</b></li> <li>• <b>Firefox</b></li> <li>• <b>Internet Explorer</b></li> <li>• <b>Opera</b></li> <li>• <b>Safari</b></li> <li>• <b>Custom client profile</b></li> </ul>
Max Transactions	The maximum number of application iterations per connection. The default value is <b>1</b> .
HTTP version	Select the version of the HTTP protocol to be used on the client side from the available options: <ul style="list-style-type: none"> <li>• <b>HTTP/1.1 (default option)</b></li> <li>• <b>HTTP/1.0</b></li> <li>• <b>HTTP/2</b></li> </ul>

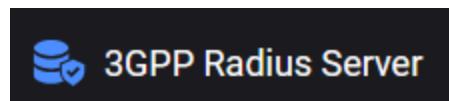
Parameter	Description
	<p><b>NOTE</b> The HTTP/2 version is supported only for the HTTP App. It is not supported for the other types of applications, nor for attacks.</p> <p>To configure HTTP/2 version for the HTTP App, select the HTTP/2 version at the application profile level (<b>Application Profile Configuration &gt; HTTP Settings &gt; HTTP Version</b>). To run a test with applications that have both HTTP/2 version (for the HTTP App) and HTTP/1.X version enabled (for other applications), make sure the <b>Inherit HTTP</b> option is disabled at the level of the other applications. To disable the <b>Inherit HTTP</b> option at an application level:</p> <ol style="list-style-type: none"> <li>1. Under <b>Application Profile Configuration</b>, select the <b>Applications</b> tab.</li> <li>2. Select the <b>Advanced Settings</b> gear menu (⚙️) for the other application(s) used in the test.</li> <li>3. On the <b>Application Settings</b> page that opens, under the <b>HTTP Settings</b> tab, disable the <b>Inherit HTTP</b> option using the toggle.</li> </ol>
Connection persistence	Configure the connection persistence mode. The available options are: <ul style="list-style-type: none"> <li>• <b>Standard</b> (default option) - This mode inherits the behavior as described by the selected HTTP version standard.</li> <li>• <b>Disabled</b> - This mode forces the connection to close after every HTTP message.</li> <li>• <b>Enabled</b> - This mode enforces connection persistence through explicit keep-alive frames.</li> </ul>
Headers	Add, delete, or customize the headers that the client will send.

## Server HTTP Settings

Parameter	Description
<i>Server HTTP Settings</i>	
HTTP profile	Select the server HTTP profile from the available options: <ul style="list-style-type: none"> <li>• <b>Apache</b> (default option)</li> <li>• <b>IIS</b></li> <li>• <b>nginx</b></li> <li>• <b>Custom server profile</b></li> </ul>
HTTP version	Select the version of the HTTP protocol to be used on the client side from the available options:

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>HTTP/1.1 (default option)</b></li> <li>• <b>HTTP/1.0</b></li> <li>• <b>HTTP/2</b></li> </ul> <p><b>NOTE</b> The HTTP/2 version is supported only for the HTTP App. It is not supported for the other types of applications, nor for attacks.</p> <p>To configure HTTP/2 version for the HTTP App, select the HTTP/2 version at the application profile level ( <b>Application Profile Configuration &gt; HTTP Settings &gt; HTTP Version</b>). To run a test with applications that have both HTTP/2 version (for the HTTP App) and HTTP/1.X version enabled (for other applications), make sure the <b>Inherit HTTP</b> option is disabled at the level of the other applications. To disable the <b>Inherit HTTP</b> option at an application level:</p> <ol style="list-style-type: none"> <li>1. Under <b>Application Profile Configuration</b>, select the <b>Applications</b> tab.</li> <li>2. Select the <b>Advanced Settings</b> gear menu (⚙️) for the other application(s) used in the test.</li> <li>3. On the <b>Application Settings</b> page that opens, under the <b>HTTP Settings</b> tab, disable the <b>Inherit HTTP</b> option using the toggle.</li> </ol>
Connection persistence	Configure the connection persistence mode. The available options are: <ul style="list-style-type: none"> <li>• <b>Standard</b> (default option) - This mode inherits the behavior as described by the selected HTTP version standard.</li> <li>• <b>Disabled</b> - This mode forces the connection to close after every HTTP message.</li> <li>• <b>Enabled</b> - This mode enforces connection persistence through explicit keep-alive frames.</li> </ul>
Additional headers	Configure other headers that will be sent alongside the application specific headers.
Use application server headers	This option is enabled by default. When enabled, all the servers to which the current profile applies will use their specific headers from the ATI definition. When disabled, the servers will use the list of headers specified in the <b>Headers</b> parameter.
Headers	Add, delete, or customize the headers that the server will send. This section appears only if <b>Use application server headers</b> is <b>disabled</b> .

## 3GPP RADIUS Server configuration settings



3GPP Remote Authentication Dial In User Service (RADIUS) Server is an implementation of the RADIUS protocol, designed to support access control and accounting functions in mobile networks, as defined by 3GPP standards. It authenticates subscribers, authorizes network access, and performs basic accounting operations.

Supported procedures are Authentication, Accounting Start and Accounting Stop.

The configuration settings are described in the topics listed below.

### Topics:

<b>3GPP RADIUS Server Ranges panel</b>	<b>275</b>
<b>3GPP RADIUS Server Range settings</b>	<b>276</b>
<b>3GPP RADIUS Server Node settings</b>	<b>277</b>
<b>3GPP RADIUS Server N6 interface settings</b>	<b>277</b>

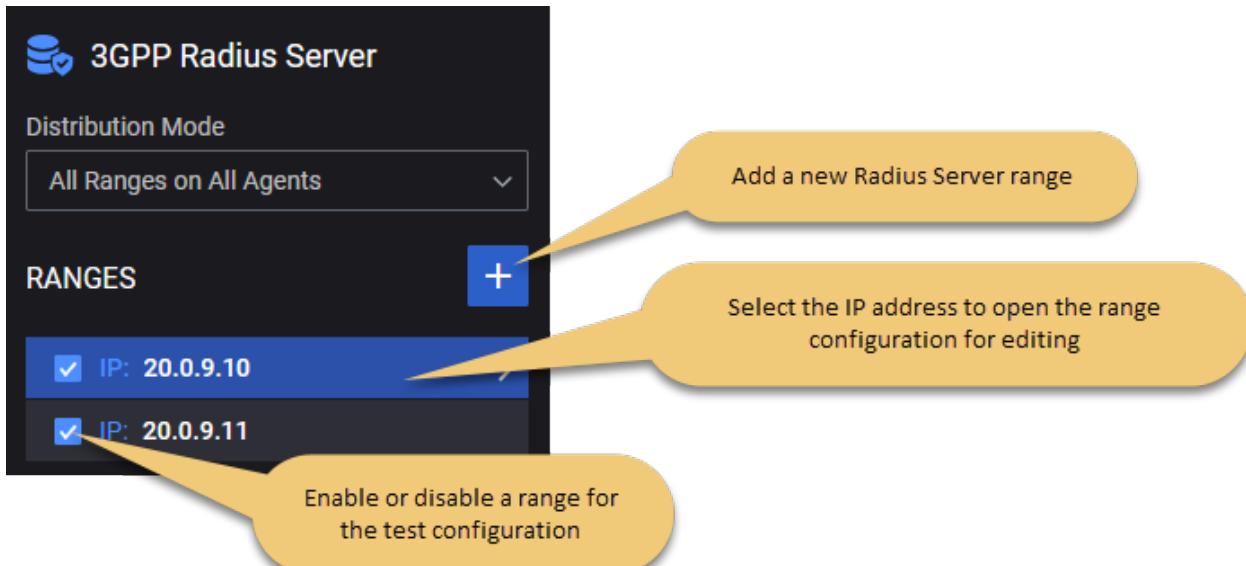
### 3GPP RADIUS Server Ranges panel

The **3GPP RADIUS Server Ranges** panel opens when you select the RADIUS Server node from the network topology window.

You can perform the following tasks from this panel:

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

#### For example ...



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All Ranges on All Agents** - This setting will configure all RADIUS Sever ranges on all agents. It will increment RADIUS N6 IP address on each agent.

## 3GPP RADIUS Server Range settings

You add and select 3GPP RADIUS Server ranges from the 3GPP RADIUS Server Ranges panel. When you select the name of a RADIUS Server, LoadCore opens the **Range** panel, from which you can:

- Delete the 3GPP RADIUS Server 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 3GPP RADIUS Server range.

### 3GPP RADIUS Server range controls and settings

Each RADIUS Server 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 RADIUS Server range.

Setting	Description
<i>Range:</i>	
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
Device Under Test	Enable this option if your RADIUS Server is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the RADIUS Server functionality (if it is selected in the Topology window).
Range Count	The number of RADIUS Servers in the 3GPP RADIUS Server range.
<i>Range Settings:</i>	
Node Settings	Each RADIUS Server range requires the configuration of an associated set of Node Settings, which are described in <a href="#">3GPP RADIUS Server Node settings</a> .
N6 Interface Settings	The RADIUS Server range requires the configuration of N6 interface settings (this interface is used for SIP). These settings are described in <a href="#">3GPP RADIUS Server N6 interface settings</a> .

## 3GPP RADIUS Server Node settings

Each 3GPP RADIUS Server range includes a set of Node Settings.

### Node Settings

Each 3GPP RADIUS Server instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Name	The name uniquely identifies each SMF instance. You can accept the value provided by LoadCore or overwrite it with your own value.
Authentication Port	RADIUS Authentication UDP port number used by the 3GPP RADIUS Server.
Accounting Port	RADIUS Accounting UDP port number used by the 3GPP RADIUS Server.
UDP Rx Buffer (bytes)	The size in bytes of the receive buffers for UDP sockets: <ul style="list-style-type: none"> <li>minimum: 212992</li> <li>maximum: 134217728</li> <li>default: 12582912</li> </ul>
UDP Tx Buffer (bytes)	The size in bytes of the transmit buffers for UDP sockets: <ul style="list-style-type: none"> <li>minimum: 212992</li> <li>maximum: 134217728</li> <li>default: 2097152</li> </ul>

## 3GPP RADIUS Server N6 interface settings

N6 is the service-based interface through which a 3GPP RADIUS Server instance makes its services available to other services in a 5G network.

The following **Connectivity Settings** enable the necessary 3GPP RADIUS Server N6 connectivity and service interaction.

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix that has been assigned to this node.
IP Address Increment	Set the IP address increment value.

<b>Connectivity Settings</b>	<b>Description</b>
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.
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
<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 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.
Gateway Address	The IP address assigned as 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner</i></p>

<b>Connectivity Settings</b>	<b>Description</b>
	<i>VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

# 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:

<b>AMF Ranges panel</b> .....	<b>281</b>
<b>AMF Range settings</b> .....	<b>282</b>
<b>AMF Node settings</b> .....	<b>283</b>
<b>AMF Custom NF Services settings</b> .....	<b>286</b>
<b>AMF N2 interface settings</b> .....	<b>287</b>
<b>AMF Namf interface settings</b> .....	<b>290</b>
<b>AMF N26 Interface Settings</b> .....	<b>292</b>
<b>AMF Remote SBA nodes</b> .....	<b>293</b>

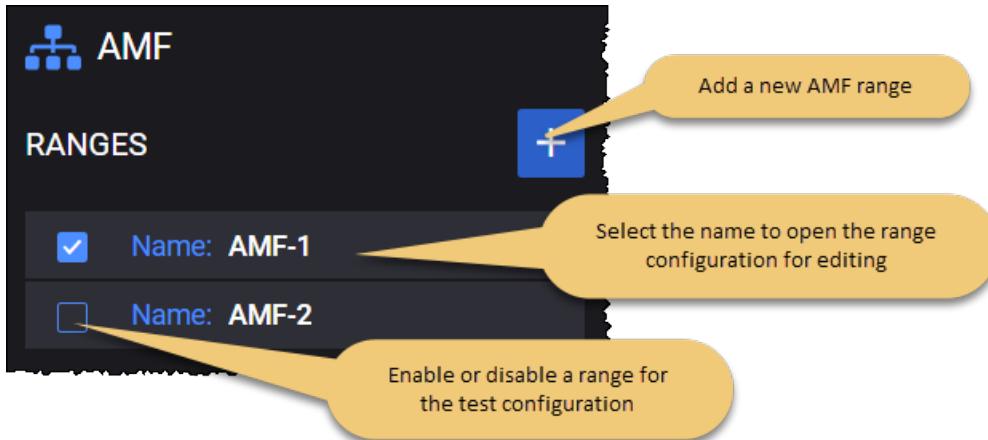
## AMF Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All Ranges on All Agents** - This setting will configure all AMF ranges on all agent. It will increment IP addresses, AMF pointer, NF ID, etc. for each agent.

## 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 <b>Delete Range</b> 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 <a href="#">AMF node settings</a> .
Custom NF Services	<p><b>IMPORTANT</b> This option appears if the range is set as DUT.</p> <p>This option will allow the configuration of a list of service parameters. See <a href="#">AMF Custom NF Services settings</a> for more information.</p>
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 <a href="#">AMF N2 interface settings</a> .
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 <a href="#">AMF Namf interface settings</a> .
N26 Interface Settings	In a 5G network, N26 is the interface between the MME and the AMF. These settings are described in <a href="#">AMF N26 Interface Settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">AMF remote SBA nodes</a> .

Setting	Description
TLS Server Name	<p><b>IMPORTANT</b> This option appears only if the range is set as DUT.</p> <p>The name of the server to be sent in SNI extension header in TLS Client Hello message.</p>

## 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>
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
Name	The name uniquely identifies each AMF instance. 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><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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	An AMF Region consists of one or multiple AMF Sets.

<b>Setting</b>	<b>Description</b>
	The AMF Region ID to use for this simulated AMF node. This ID identifies the region in which the node resides. The AMF Region ID addresses the case that there are more AMFs in the network than the number of AMFs that can be supported by AMF Set ID and AMF Pointer. It allows operators to re-use the same AMF Set IDs and AMF Pointers in different regions.
Set ID	<p>An AMF Set consists of some AMFs that serve a given area and Network Slice. Multiple AMF Sets may be defined per AMF Region and Network Slice(s).</p> <p>The AMF Set ID to use for this simulated AMF node. The Set ID uniquely identifies the AMF Set within the AMF Region.</p>
Pointer	The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.
Relative Capacity	Set the relative capacity value.
Ciphering Algorithm	<p>Allows to select the supported 5G ciphering algorithm:</p> <ul style="list-style-type: none"> <li>• NEA0 - Null ciphering algorithm</li> <li>• NEA1 - 128-bit SNOW 3G based algorithm</li> <li>• NEA2 - 128-bit AES based algorithm</li> </ul>
Integrity Algorithm	<p>Allows to select the supported 5G integrity protection algorithm:</p> <ul style="list-style-type: none"> <li>• NIA0 - Null Integrity Protection algorithm</li> <li>• NIA1 - 128-bit SNOW 3G based algorithm</li> <li>• NIA2 - 128-bit AES based algorithm</li> </ul>
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	<p>Enable this option to trigger Establishment of UE Policy Association to PCF.</p> <div data-bbox="442 1474 633 1537" style="background-color: #e0e0e0; padding: 5px; border-radius: 5px; display: inline-block;">NOTE</div> <p>UE Policy Association is not supported in tests configured with Idle or Handover objectives.</p> <div data-bbox="442 1548 633 1611" style="background-color: #e0e0e0; padding: 5px; border-radius: 5px; display: inline-block;">NOTE</div> <p>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.
Roaming Type	<p>Select the roaming type option from the drop-down list: <b>None</b> or <b>Home-Routed</b>.</p> <p>Default value: <b>None</b>.</p>

Setting	Description
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
Cache NRF Response	<p><b>IMPORTANT</b> This option appears only if the NRF node is enabled and the <b>Peer NRF</b> value under <a href="#">Remote SBA Nodes &gt; NRF Connections Settings</a> is set.</p> <p>Select from the drop-down for how long to save/remember the peer SBA nodes that are discovered via NRF:</p> <ul style="list-style-type: none"> <li>• <b>Cache Permanently</b> (default)</li> <li>• <b>Don't Cache Responses</b></li> </ul>

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

<b>NOTE</b>	<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 <a href="#">below</a>.</i>
TAI	<i>These settings are described <a href="#">below</a>.</i>

## NSSAI

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

Setting	Description									
<b>NSSAI:</b>										
	Select the Add NSSAI button to add a new NSSAI to your test configuration.									
<b>NSSAI settings:</b>										
	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> </tbody> </table>	SST	Value	Suitable for handling:	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications
SST	Value	Suitable for handling:								
eMBB	1	5G enhanced Mobile Broadband								
URLCC	2	ultra-reliable low-latency communications								

<b>Setting</b>	<b>Description</b>		
	<b>SST</b>	<b>Value</b>	<b>Suitable for handling:</b>
	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.

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

## AMF Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## 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
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).
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
Additional Routes	The additional routes will use the gateway defined in the IP information below.

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

The **Additional Addresses** section allows setting additional AMF N2 interface IP addresses used for multihoming.

<b>Settings</b>	<b>Description</b>
<i>Additional Addresses</i>	
	Select this button to add an additional address to your test configuration.
	Select this button to remove the additional address from your test configuration.
<i>Connectivity Settings</i>	

<b>Settings</b>	<b>Description</b>
<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).
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
<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 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.
Gateway Address	The IP address assigned as gateway address.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i> ). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## AMF Namf interface settings

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

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

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix 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 <b>HTTP</b> or <b>HTTPS</b> .
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.
Gateway Address	The IP address assigned as 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.

Connectivity Settings	Description
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

The following **Security Settings** enable the necessary Namf security interaction.

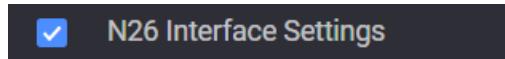
Security Settings	Description
<i>TLS Settings</i>	
mTLS Client Settings	Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</p>
CA Certificate	Select from the drop-down list one of the available server certificates.
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRTand the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>

Security Settings	Description
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.
	<p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## 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.
GTP-C	Specify the UDP port that will be used for GTP-C message transmission. Value

Setting	Description
Destination UDP Port	should be in range of 1024 to 65535.

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

## 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.
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-

Setting	Description
	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"> <li>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.</li> <li>Select <b>Discover</b> to invoke the NF discovery service. Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</li> </ul>
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	<b>IMPORTANT</b> This option is visible only when SCP is selected in SCP Connection Settings. Select the option to enable it. For more details, refer to <a href="#">Indirect Communication without Delegated Discovery</a> .
Indirect Communication with Delegated Discovery	<b>IMPORTANT</b> This option is visible only when Peer AUSF is set to <b>Discover</b> and SCP is selected in SCP Connection Settings. Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a> .

## 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.

<b>Setting</b>	<b>Description</b>
Peer UDM	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> 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><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer UDM is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a>.</p>

## PCF Connection Settings

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

<b>Setting</b>	<b>Description</b>
<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"> <li>• 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.</li> <li>• Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>

Setting	Description
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"> <li>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.</li> <li>Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nsmf communications. It can be either HTTP or HTTPS.
Port	The SMF port number to use for Nsmf communications. The default is port 80, but you can choose a different port number.
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer SMF is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a>.</p>

## NRF Connection Settings

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

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

## DNS Server Connection Settings

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.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

## 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"> <li>• <b>Telescopic FQDN</b></li> <li>• <b>Target API Root</b></li> </ul>

## Home PLMN for Inter-PLMN Routing

The following configuration settings are required.

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

	<p>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:

<b>AUSF Ranges panel</b> .....	<b>302</b>
<b>AUSF Range panel</b> .....	<b>302</b>
<b>AUSF Node settings</b> .....	<b>303</b>
<b>AUSF Nausf interface settings</b> .....	<b>304</b>
<b>AUSF Remote SBA Nodes</b> .....	<b>307</b>
<b>AUSF Custom NF Services settings</b> .....	<b>309</b>

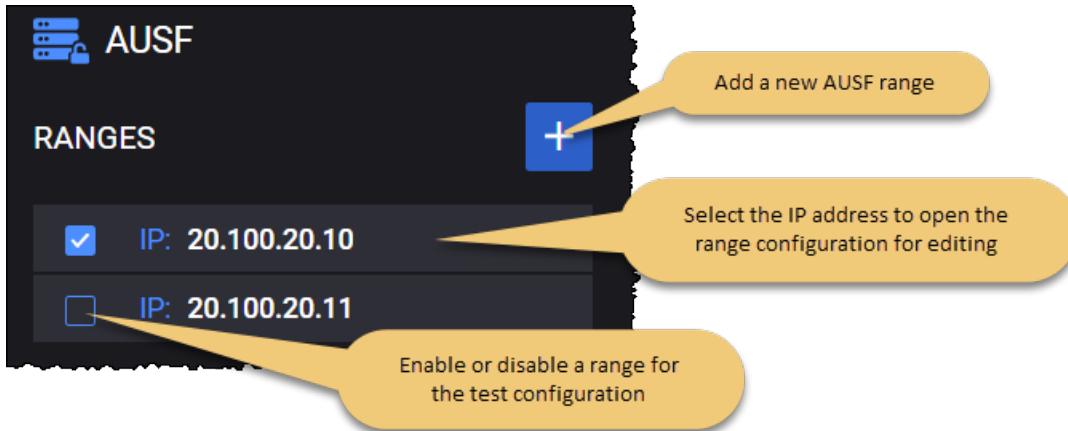
## AUSF Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT** Only one AUSF range can be configured on one agent:

- in case of multiple ranges, it will require one agent for each range;
- in case one range and multiple agents, each agent will create a different AUSF NF, with incremented IP address and NF ID, and whole UE range.

## 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 <b>Delete Range</b> 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).
<i>Range Settings (when range is not set as DUT):</i>	
Node Settings	Each AUSF range includes the configuration of an associated set of Node Settings, which are described in <a href="#">AUSF node settings</a> .
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 <a href="#">AUSF Nausf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">AUSF remote SBA nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nausf IP Address	The IP address from your test network to use for traffic on this interface.
Custom NF Services	This option will allow the configuration of a list of service parameters. See <a href="#">AUSF Custom NF Services settings</a> for more information.
TLS Server Name	The name of the server to be sent in SNI extension header in TLS Client Hello message.

## 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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.

Setting	Description
PLMN MCC	<p>Set the mobile country code.</p> <p><b>About PLMN MCC ...</b></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>Set the mobile network code.</p> <p><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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 <b>Add Routing Indicator</b> button to add a routing indicator for the AUSF range.
	Select the <b>Delete</b> 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.

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

The following **Security Settings** enable the necessary Nausf security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
<i>mTLS Client Settings</i>	<i>Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.</i>
<i>Certificates and Private Keys (.zip)</i>	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Role Name</i>	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>mTLS Server Settings</i>	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
<i>CA Certificate</i>	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Certificates and Private Keys (.zip)</i>	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Role Name</i>	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>Use Secrets Management System</i>	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p>

Security Settings	Description
	<p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.
	<p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## AUSF Remote SBA Nodes

### UDM Connection Settings

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

Setting	Description
<i>UDM Connection Settings:</i>	
Peer UDM	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> 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><b>IMPORTANT</b> This option is visible only when SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it.</p>

Setting	Description
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer UDM is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p> <p>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>	
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.

**DNS Server Connection Settings**

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.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

**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.

## AUSF Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## 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:

<b>CHF Ranges panel</b>	<b>310</b>
<b>CHF Range settings</b>	<b>311</b>
<b>CHF Node settings</b>	<b>312</b>
<b>CHF Nchf interface settings</b>	<b>313</b>
<b>CHF remote SBA nodes</b>	<b>315</b>

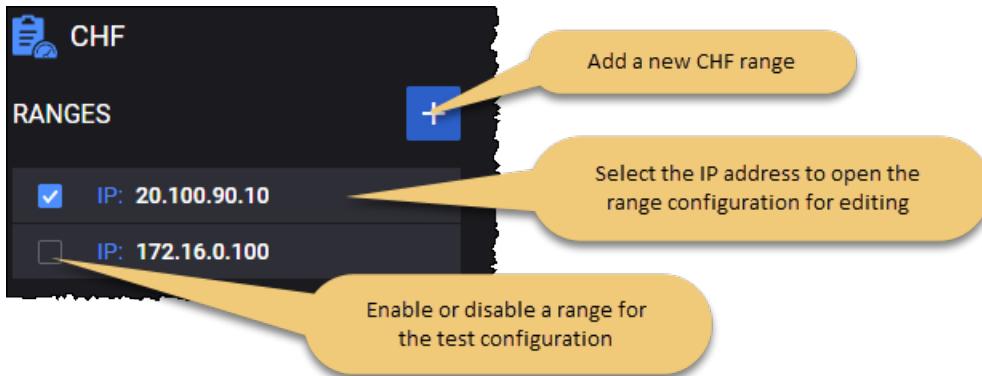
### CHF Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT** Only one CHF range can be configured on one agent:

- in case of multiple ranges, it will require one agent for each range;
- in case one range and multiple agents, each agent will create a different CHF NF, with incremented IP address and NF ID, and whole UE range.

## 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
Range:	

Setting	Description
	Select the <b>Delete Range</b> 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 (when range is not set as DUT):</i>	
Node Settings	Each CHF range requires the configuration of an associated set of Node Settings, which are described in <a href="#">CHF node settings</a> .
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 <a href="#">CHF Nchf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">CHF remote SBA nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nchf IP Address	The IP address from your test network to use for traffic on this interface.

## 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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
PLMN MCC	The PLMN MCC for this AMF range. <b>About PLMN MCC ...</b> 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

Setting	Description
	<p>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><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix that has been assigned to this node.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Protocol	The protocol to use for this interface communications. You can choose either HTTP or HTTPS.
Port	The TCP port number to use for this interface communications. The default is port 80, but you can choose a different port number.
<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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

The following **Security Settings** enable the necessary Nchf security interaction.

Security Settings	Description
<i>TLS Settings</i>	
mTLS Client Settings	Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</p>
CA Certificate	Select from the drop-down list one of the available server certificates.
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRTand the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>

Security Settings	Description
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings, other then the one selected in Active Root Certificate.</p> <p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## CHF remote SBA nodes

### NRF Connection Settings

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

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

## SCP Connection Settings

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

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

# 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:

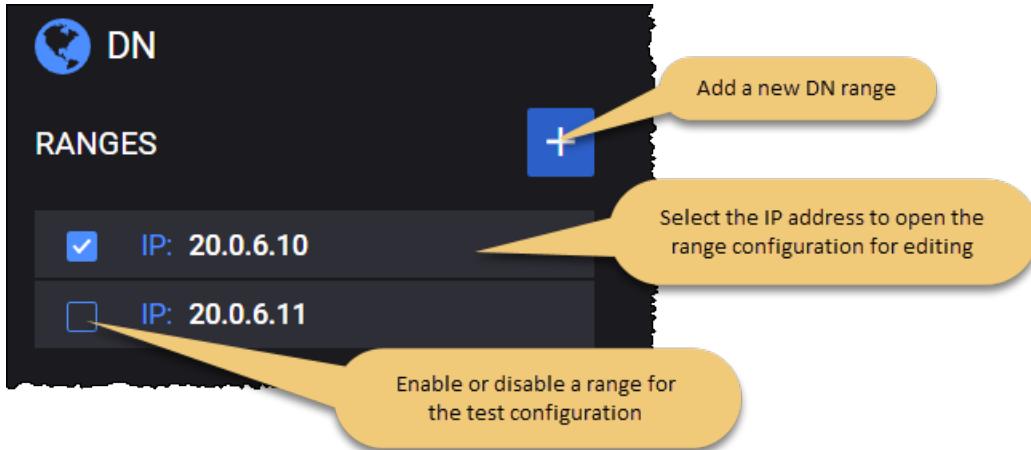
<b>DN Ranges panel</b>	<b>318</b>
<b>DN Range panel</b>	<b>318</b>
<b>DN N6 interface settings</b>	<b>319</b>
<b>DN routes settings</b>	<b>320</b>
<b>DN User Plane</b>	<b>321</b>
DN Stateless UDP Traffic	322
DN Data Traffic	324
DN Voice Traffic	326
DN Video OTT Traffic	337
DN DNS Server Traffic	340
DN Predefined Applications Traffic	343
DN Capture Replay	343
DN Synthetic	345
DN UDG	347
<b>DN Throttling settings</b>	<b>349</b>

## 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 ...**



If multiple agents are assigned to the DN node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **All Ranges on All Agents**

## 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 <b>Delete Range</b> 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 <a href="#">DN N6 interface settings</a> .
Routes Settings	These settings are described in <a href="#">DN routes settings</a> .
User Plane	These settings are described in <a href="#">DN User Plane</a> .
Throttling Settings	These settings are described in <a href="#">DN Throttling settings</a> .

## 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
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

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

## DN routes settings

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

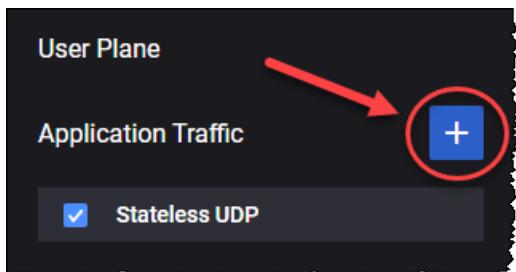
The following table describes the **Route Settings** that you need to configure in order to create the route to an UE or custom range.

<b>Settings</b>	<b>Description</b>
<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: <b>UE</b> or <b>Custom</b> .
UE Range MSIN	Select the MSIN of the UE range from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .

Settings	Description
Peer UPF	Select the UPF node connected to DN over the N6 interface from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .
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"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> This parameter is available only when the route type is set to <b>UE</b> .
Destination Subnet Address	Set the destination subnet address. This parameter is available only when the route type is set to <b>Custom</b> .
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 <b>Custom</b> .

## 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"> <li>• <b>Stateless UDP</b></li> <li>• <b>Data</b></li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>Voice</b></li> <li>• <b>Video OTT</b></li> <li>• <b>DNS Server</b></li> <li>• <b>Predefined Applications</b></li> <li>• <b>Synthetic</b></li> <li>• <b>UDG</b></li> </ul>
	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 <a href="#">DN Stateless UDP Traffic</a> .
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">DN Data Traffic</a> .
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">DN Voice Traffic</a> .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">DN Video OTT Traffic</a> .
DNS Server	For the settings required to configure the DNS Server objective, refer to <a href="#">DN DNS Client Traffic</a> .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to <a href="#">DN Predefined Applications Traffic</a> .
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to <a href="#">DN Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG traffic objective, refer to <a href="#">DN UDG Traffic</a> .

## 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 <b>Stateless UDP</b> .
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 <b>dowlink</b> 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.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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 <b>Data</b> .
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"> <li>• To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.</li> <li>• To add another application server, click the <b>Add Server</b> button. LoadCore will open the Server panel where you will select the server type and configure the server settings.</li> </ul> <p>Refer to <a href="#">Server</a> (below) for a description of the configuration settings required by the application server.</p> <p>Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Server</b> 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: <b>TCP</b> , <b>TLS</b> , <b>QUIC</b> or <b>UDP</b> .
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"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get Responder</b>, <b>HTTP Put Responder</b>, <b>HTTP Post Responder</b>, <b>HTTP Server</b> and <b>FTP Responder</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get Responder</b>, <b>HTTPS Put Responder</b>, <b>HTTPS Post Responder</b> and <b>HTTPS Server</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Server</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional Responder</b>.</li> </ul>
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. <div style="margin-left: 20px;"> <b>NOTE</b> Setting the page size on DN side will only influence GET objectives, like HTTP GET, HTTPs GET and FTP. To set the page size for PUT objectives, the change must be operated on UE side.           </div>
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

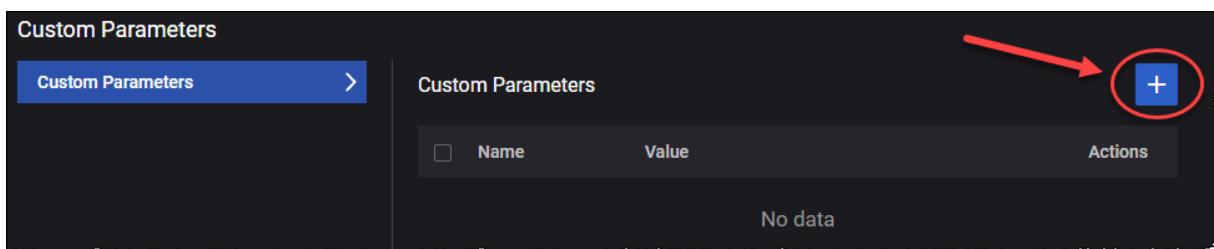
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

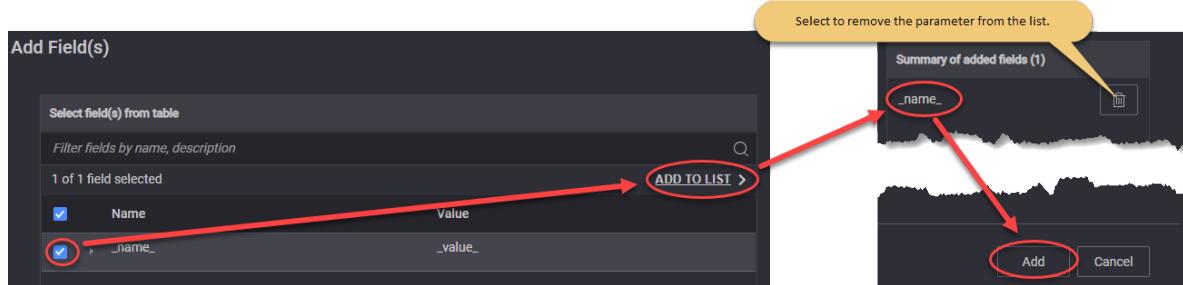
2. Select the **Add** button.



The Add Field(s) opens.

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 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 <b>Voice</b> .
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 <b>Simulated Users</b> and cannot be changed.
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 <a href="#">Dial Plan</a>.</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"> <li>• <b>TCP</b> - Transmission Control Protocol</li> <li>• <b>TLS</b> - Transport Layer Security</li> <li>• <b>UDP</b> - User Datagram Protocol</li> </ul>

Parameter	Description
Domain	Provide the domain name.
Advanced SIP Settings	For more details about these settings, refer to <a href="#">Advanced SIP Settings</a> .
<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.
Enable SRTP	Select this option in order to enable Secure Real-time Transport Protocol (SRTP).
RTP Session Duration (ms)	Set the value for the session duration.
Audio settings:	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
Video Settings:	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
MSRP Settings:	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
MCTTP Settings	<i>For the configuration of MCTTP settings, refer to <a href="#">MCPTT Settings</a>.</i>
<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"> <li>• <b>None</b></li> <li>• <b>EVS/AMR IPv4</b></li> <li>• <b>NB Codecs IPv6</b></li> <li>• <b>AMR-WB IPv6</b></li> <li>• <b>Multimedia IPv4</b></li> </ul>
QoE Settings	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

## Dial Plan

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

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

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Voice	Select the QoS flow used for voice 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"> <li>• <b>AMR</b> - 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.</li> <li>• <b>AMR-WB</b> - 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.</li> <li>• <b>EVS</b> - 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.</li> <li>• <b>PCMU</b></li> <li>• <b>PCMA</b></li> <li>• <b>iLBC</b></li> </ul>

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

### AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth efficient:</b> In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added.</li> <li>• <b>Octet aligned:</b> 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.</li> </ul>
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"> <li>• <b>Full header</b> - 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.</li> <li>• <b>Compact</b> - In this payload format a single codec data frame is sent in each RTP packet. The format uses protected payload sizes that uniquely identify</li> </ul>

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

### PCMU/PCMA/iLBC/G722/G723/G729

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

### Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Voice	Select the QoS Flows ID(s) from the drop-down list.
Video Codecs	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

### MSRP Settings

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

Parameter	Description
Enable MSRP	Select to enable this option.

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

## MCPTT Settings

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

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

## Advanced SIP Settings

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

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

### SIP Custom Headers

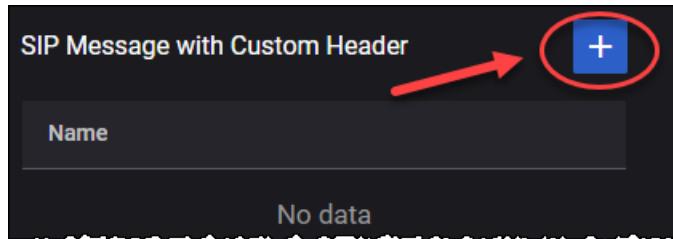
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

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

For each message, you can:

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

- Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**

The following custom header are available:

Parameter	Description	Value
Accept	IETF RFC 3261	application/sdp,message/cpim
Accept-Contact	IETF RFC 3841	*;mobility="mobile";methods="INVITE"
Accept-Encoding	IETF RFC 3261	gzip
Accept-Language	IETF RFC 3261	da, en-gb;q=0.8, en;q=0.7
Alert-Info	IETF RFC 3261	:<urn:alert:service:call-waiting>
Allow	IETF RFC 3261	INVITE, ACK, UPDATE, PRACK, CANCEL, PUBLISH, MESSAGE, OPTIONS, SUBSCRIBE, NOTIFY

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
Allow-Events	IETF RFC 6665	conference
Authentication-Info	IETF RFC 3261, IETF RFC 3310	nexnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	<http://www.example.com/alice/photo.jpg> ;purpose=icon
Content-Disposition	IETF RFC 3261	session
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:0 0 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC 3261	3600
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC	<user1@operator1.com>

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
n	IETF RFC 3261	6442
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-Associate-d-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

Parameter	Description	Value
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmTEL
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=False,algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>, <sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org?Replaces=425928%40bobster.example.com.3%3Btag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path

Parameter	Description	Value
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
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"> <li>• <b>Digest MD5</b></li> <li>• <b>AKAv1</b></li> <li>• <b>AKAv2</b></li> <li>• <b>ProxyDefined</b></li> </ul>
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 <b>Video OTT</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it

Parameter	Description
	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).
<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"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Streams</a> (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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.

Parameter	Description
	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"> <li>• <b>Real</b></li> <li>• <b>Synthetic</b></li> </ul>
Protocol	Select the protocol from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Apple HLS</b></li> <li>• <b>DASH</b>.</li> </ul> If the stream type is set to <b>Synthetic</b> , you can choose one protocol from list. If the stream type is set to <b>Real</b> , you will see the protocol of real stream loaded.
Stream Duration	If the stream type is set to <b>Synthetic</b> , you can configure the stream duration in seconds. If the stream type is set to <b>Real</b> , you will see the real stream duration.
Segment Duration	If the stream type is set to <b>Synthetic</b> , you can configure the segment duration in seconds. If the stream type is set to <b>Real</b> , 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: <b>QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K</b> .
Frames per second	Set the number of frames per second.

## Custom Parameters

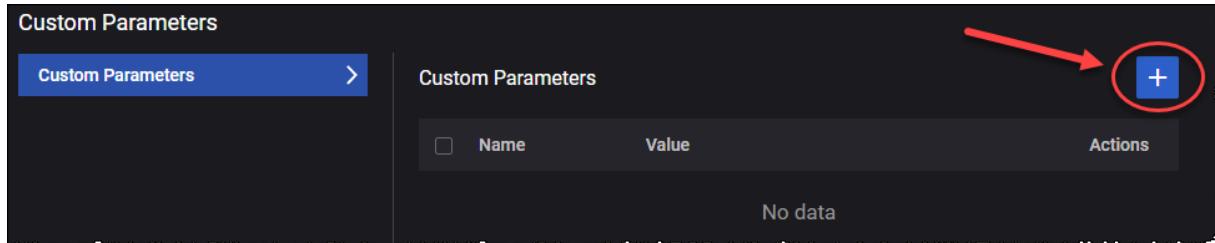
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

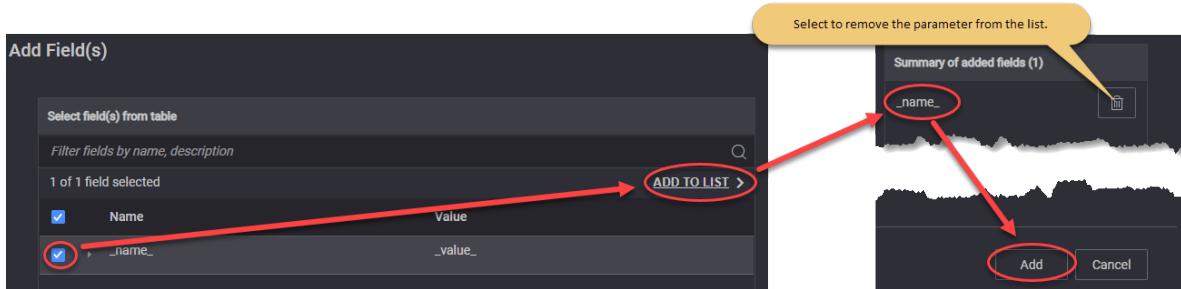
2. Select the **Add** button.



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 <b>DNS Server</b> .
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).

Parameter	Description
<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 <a href="#">Zone Manager</a> (below) for descriptions of the DNS server zones settings.</i>
Custom Parameters	<i>You can add <a href="#">custom parameters</a>, 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.

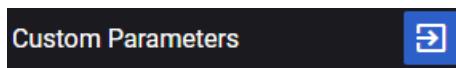
Parameter	Description
	Select this button to add a zone to your test configuration.
	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by LoadCore or overwrite it with your own value.
Master Server	Provide the value for the master server.
Resource Records (RRs)	
	Select this button to add a resource record to your test configuration.

Parameter	Description
	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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
Hostname	Set the hostname.
Address	Provide the address.

## Custom Parameters

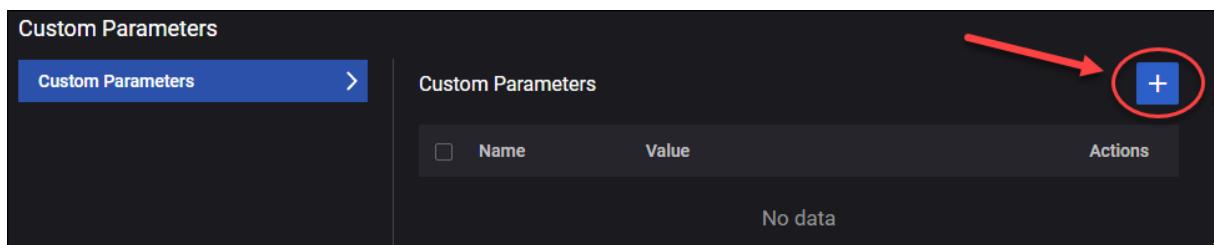
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

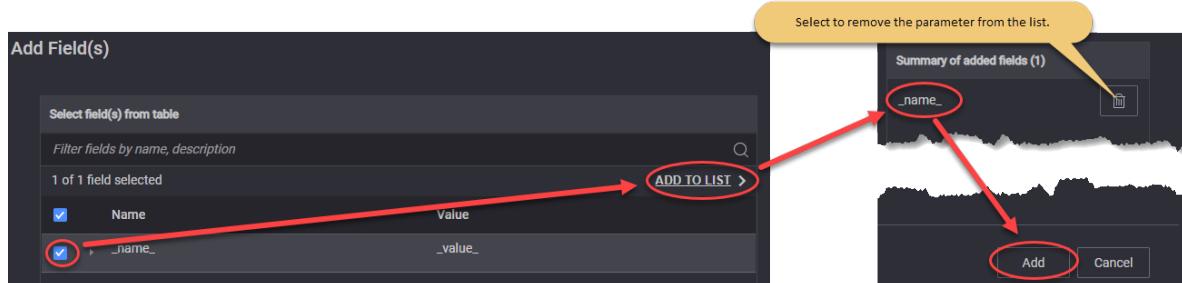
2. Select the **Add** button.



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 <b>Predefined Applications</b> .
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 <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b>

Parameter	Description
	(option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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: <b>Initiator</b> and <b>Responder</b> .

Parameter	Description
	Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> (option disabled).
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to <b>Initiator</b> . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

## DN Synthetic

The following table describes the Synthetic parameters.

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

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

The following table describes the Traffic Flow parameters.

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

## DN UDG

The following table describes the UDG parameters.

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

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

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

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

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

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

## DN Throttling settings

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

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

**NOTE**

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

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

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

## DNS Server configuration settings



LoadCore includes simulation and isolation for DNS Server node.

The configuration settings are described in the topics listed below.

### Topics:

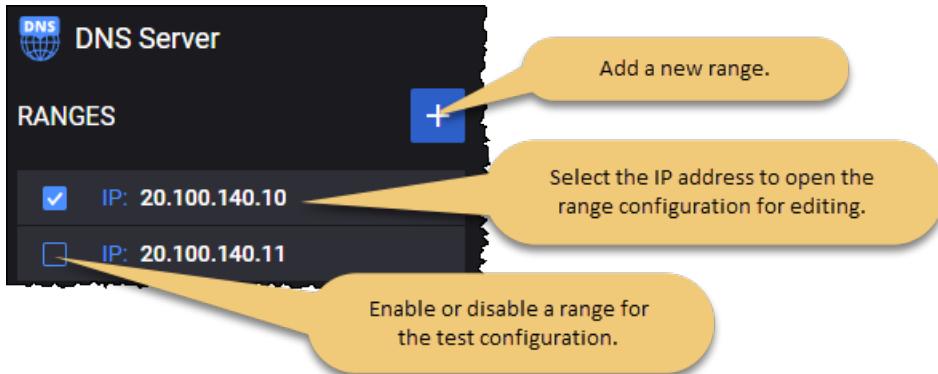
<b>DNS Server Ranges panel</b>	350
<b>DNS Server Range panel</b>	350
<b>DNS Server Ndnsserver interface settings</b>	351
<b>DNS Server Traffic Flow settings</b>	352

### 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 <b>Delete Range</b> 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 <a href="#">DNS Server Ndnsserver interface settings</a> .
Traffic Flow Settings	These settings are described in <a href="#">DNS Server Traffic Flow settings</a> .

## 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.

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

## DNS Server Traffic Flow settings

The following table describes the DNS Server Traffic Flow parameters.

<b>Parameter</b>	<b>Description</b>
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Zone Manager	Refer to <a href="#">Zone Manager</a> (below) for descriptions of the DNS server zones settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
Hostname	Set the hostname.
Address	Provide the address.

## Custom Parameters

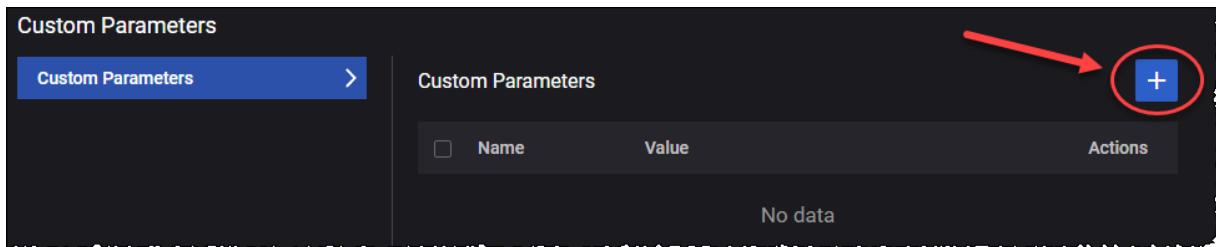
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

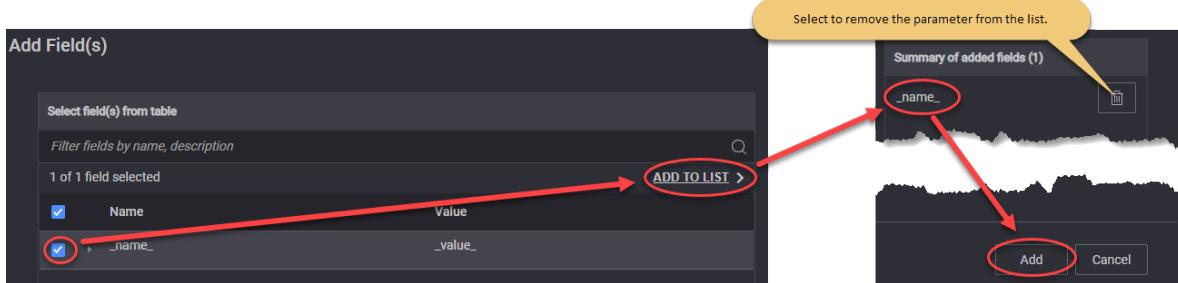
2. Select the **Add** button.



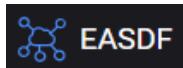
The Add Field(s) opens.

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 ...**



# EASDF configuration settings



Edge Application Server Discovery Function (EASDF) is the application by which a UE discovers the IP address(es) of a suitable Edge Application Server(s) using Domain Name System (DNS).

Within the 5GC, the EASDF offers services to the SMF via the Neasdf service based interface (see 3GPP TS 23.548 [14], 3GPP TS 23.501 [2] and 3GPP TS 23.502 [3]).

**IMPORTANT** EASDF is disabled by default in the topology. When enabled, make sure that **Technical Spec version** is set to **R17 December 2022** in Global Settings .

The configuration settings are described in the topics listed below.

## Topics:

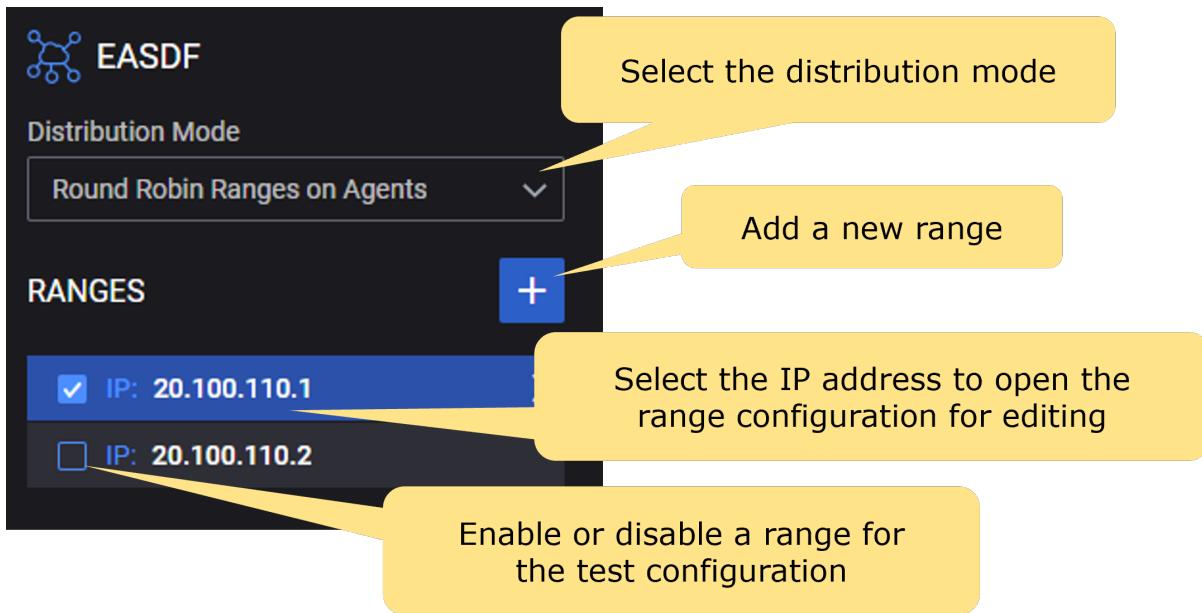
<b>EASDF Ranges panel</b>	<b>355</b>
<b>EASDF Range panel</b>	<b>356</b>
<b>EASDF Node settings</b>	<b>357</b>
<b>EASDF Neasdf interface settings</b>	<b>357</b>
<b>EASDF N6 interface settings</b>	<b>360</b>
<b>EASDF UE routes settings</b>	<b>360</b>
<b>EASDF DNS Server Settings</b>	<b>361</b>
<b>EASDF Custom NF Services settings</b>	<b>362</b>

## EASDF Ranges panel

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

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

**For example ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on One Agent** - This mode allows only one agent in the assignment.

**IMPORTANT** The number of enabled EASDF ranges must be equal to the number of assigned agents.

## EASDF Range panel

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

- Select the **Delete Range** button to delete the selected EASDF 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 EASDF range.

### EASDF range controls and settings

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

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

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

Setting	Description
	When this option is not enabled, the LoadCore will simulate the EASDF functionality (if it is selected in the Topology window).
<i>Range Settings:</i>	
Node Settings	Each range requires the configuration of an associated set of Node Settings, which are described in <a href="#">EASDF Node settings</a> . <b>IMPORTANT</b> If the range is set as <b>Device Under Test</b> , this setting will not be available.
Neasdf Interface Settings	Each EASDF range requires the configuration of Neasdf interface settings, through which an EASDF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in <a href="#">EASDF Neasdf interface settings</a> .
N6 Interface Settings	The EASDF range requires the configuration of N6 interface settings. These settings are described in <a href="#">EASDF N6 interface settings</a> .
UE Routes Settings	These settings are described in <a href="#">EASDF UE routes settings</a> .
DNS Server Settings	These settings are described in <a href="#">EASDF DNS Server Settings</a> .
Custom NF Services	<b>IMPORTANT</b> This option appears if the range is set as DUT. This option will allow the configuration of a list of service parameters. See <a href="#">EASDF Custom NF Services settings</a> for more information.

## EASDF Node settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple node instances may be deployed in the 5G network. Each 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.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## EASDF Neasdf interface settings

Neasdf is the interface from other SBA nodes towards the EASDF node.

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

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

The following **Security Settings** enable the necessary Neasd security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
<i>mTLS Client Settings</i>	<i>Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.</i>
Certificates and Private Keys (.zip )	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>

<b>Security Settings</b>	<b>Description</b>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>mTLS Server Settings</i>	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
CA Certificate	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	<p>Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.</p>
Active Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.</p>
Staged Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.</p>

Security Settings	Description
	<b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.

## EASDF N6 interface settings

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

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address of the proxy DNS Server to which the Edge DNS Client UEs will send DNS queries. The proxy DNS Server will forward the queries to a local DNS Server as instructed by AF/SMF.
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	DNS Server's port. The default value is 53, but you can configure a different value.
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	<b>IMPORTANT</b> This option is visible only when the Outer VLAN 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..

## EASDF UE routes settings

The following table describes the **Route Settings** that you need to configure in order to create the route to an UE range, or manually define the route(s).

Settings	Description
<i>Routes Config:</i>	

Settings	Description
	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: <b>UE</b> or <b>Custom</b> .
UE Range MSIN	Select the MSIN of the UE range from the drop-down list.
Peer UPF	Select from the drop-down list the UPF node connected to EASDF over the N6 interface.
Gateway Address	The IP address assigned as gateway address.
Destination Subnet Address	<p>Set the destination subnet address.</p> <div style="display: flex; align-items: center;"> <span style="background-color: #004a89; color: white; padding: 2px 5px; margin-right: 5px;"><b>IMPORTANT</b></span> <span>This parameter is available only when the route type is set to <b>Custom</b>.</span> </div>
IP Prefix Length	<p>The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.</p> <div style="display: flex; align-items: center;"> <span style="background-color: #004a89; color: white; padding: 2px 5px; margin-right: 5px;"><b>IMPORTANT</b></span> <span>This parameter is available only when the route type is set to <b>Custom</b>.</span> </div>

## EASDF DNS Server Settings

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

Parameter	Description
<i>DNS Servers:</i>	
	Select this button to add a server to your test configuration.
<i>DNS Server:</i>	
	Select this button to remove the server from the test configuration.
IP Address	The IP address of the local DNS Server to which the proxy DNS Server will forward the DNS queries on behalf of Edge DNS Client UEs, as instructed by AF/SMF.
DNS Server Zones	<i>Select to configure the DNS server zones for this range.</i>

Parameter	Description
<i>Zones:</i>	
	Select this button to add a zone to your test configuration.
<i>Zone:</i>	
	Select this button to remove the selected 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.
<i>Resource Records (RRs)</i>	
	Select this button to add a resource record to your test configuration.
<i>Resource Record</i>	
	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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> </ul>
Hostname	Set the hostname for this resource.
Address	Provide the address of this resource.

## EASDF Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	

<b>Setting</b>	<b>Description</b>
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the apiRoot for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## 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:

<b>CSCF Range panel</b>	<b>364</b>
CSCF N6 interface settings	366
CSCF AF Interface settings	367
CSCF UE routes settings	370
<b>Media Function Range panel</b>	<b>370</b>

### 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.

<b>Setting</b>	<b>Description</b>
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.
Force IPsec Null Encryption	If enabled, it forces IPsec null encryption, therefore not encrypting the ESP traffic.
<i>SIP Settings</i>	
Enable Retransmission	If enabled, it will allow the independent message exchanges. A SIP transaction consists of a single request and any responses to that request. The transaction layer handles application-layer retransmissions, matching of responses to requests, and application-layer timeouts.
Enable Retransmission for TCP Transport	<p><b>IMPORTANT</b> This parameter can be enabled only if Enable Retransmission is on.</p> <p>If enabled, it will allow the message exchange for TCP transport.</p>
Timer T1 Value (ms)	T1 is an estimate of the RTT between the client and server transactions. A larger value is possible (recommended on high latency access links) if you know the RTT is larger. Default value is 500 ms.
Timer T2 Value (ms)	T2 is the maximum retransmit interval for non-INVITE requests and INVITE responses. If a provisional response is received, retransmissions continue for unreliable transports, but at an interval of T2. The default value is 4000 ms.
Timer T4 Value (ms)	T4 represents the maximum duration a message will remain in the network. The default value is 5000 ms.
Timer C Value (ms)	Time C is the proxy INVITE transaction timeout. The value must be larger than 3 minutes.
Timer D Value (ms)	Timer D represents the wait time for response retransmit.
<i>Authentication Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: <b>keysight.com</b> .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: <b>Digest</b> , <b>AKAv2</b> or <b>AKAv1</b> .
Algorithm	Select the algorithm from the drop-down list. Available options: <b>MD5</b> , <b>MD5-Sess</b> , <b>SHA256</b> or <b>SHA256-Sess</b> .
Quality of	Select an option from the drop-down list: <b>auth</b> or <b>auth-init</b> .

<b>Setting</b>	<b>Description</b>
Protection	
<i>AF Node Settings</i>	<i>The CSCF range requires the configuration of AF interface settings (this interface is used for .....). These settings are described in <a href="#">CSCF Rx interface settings</a>.</i>
<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 <a href="#">CSCF N6 interface settings</a>.</i>
<i>UE Routes Settings</i>	<i>These settings are described in <a href="#">CSCF UE routes settings</a>.</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.

<b>Interface setting</b>	<b>Description</b>
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.

<b>Connectivity Settings</b>	<b>Description</b>
<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.

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

## CSCF AF Interface settings

The following settings are required to enable AF interface transmission.

<b>Setting</b>	<b>Description</b>
<i>AF Interface settings</i>	
Use N5 instead of RX interface	If enabled, will use the N5 interface settings from the PCF node, even if PCF is set as DUT (see <a href="#">PCF Npcf interface settings</a> ).
<i>Connectivity Settings are enabling the necessary CSCF AF connectivity.</i>	
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).
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner</i></p>

<b>Setting</b>	<b>Description</b>
	<i>VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
<i>Rx Interface Settings</i>	See <a href="#">Rx Interface Settings</a> .

## 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.

<b>Setting</b>	<b>Description</b>
<i>Rx Interface Settings</i>	
Hostname	Set the hostname.
Realm	Set the realm. Default value: <b>keysight.com</b> .
Diameter Transport	Select the diameter transport type: <b>SCTP</b> or <b>TCP</b> .
<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	Set the maximum retransmissions value per path.

<b>Setting</b>	<b>Description</b>
Retransmission 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.
<i>SCTP Buffers</i>	
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the SCTP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for SCTP sockets.
<i>TCP 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.
Maximum Segment Size (MSS)	<p>The desired Maximum Segment Size (MSS) for the 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>
Use timestamps	Turn on to enable timestamps on TCP packets.
<i>TCP Buffers</i>	
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the TCP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for TCP sockets.
<i>Diameter Settings</i>	
Diameter	<i>Select to configure the Diameter settings.</i>
Set the Preliminary AAR	If enabled, the P-CSCF sends a preliminary Authorization Authentication Request (AAR) message (based on the INVITE SDP).

## CSCF UE routes settings

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

Settings	Description
<i>UE Routes Config:</i>	
	Select this button to add a new route to a specific UE range.
<i>UE Routes Config:</i>	
	Select this button to remove the route to the UE range.
UE Range MSIN	Select the MSIN of the UE range from the drop-down list.
Peer UPF	Select the UPF node connected to DN over the N6 interface from the drop-down list.
Gateway Address	The IP address assigned as gateway address.

## 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.

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

## 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:

<b>MME Ranges panel</b> .....	<b>373</b>
<b>MME Range panel</b> .....	<b>374</b>
<b>MME Node settings</b> .....	<b>375</b>
<b>MME S11 Interface Settings</b> .....	<b>377</b>
<b>MME N26 Interface Settings</b> .....	<b>378</b>
<b>MME S1 Interface Settings</b> .....	<b>380</b>
<b>MME S6a Interface Settings</b> .....	<b>381</b>
<b>MME Diameter settings</b> .....	<b>384</b>

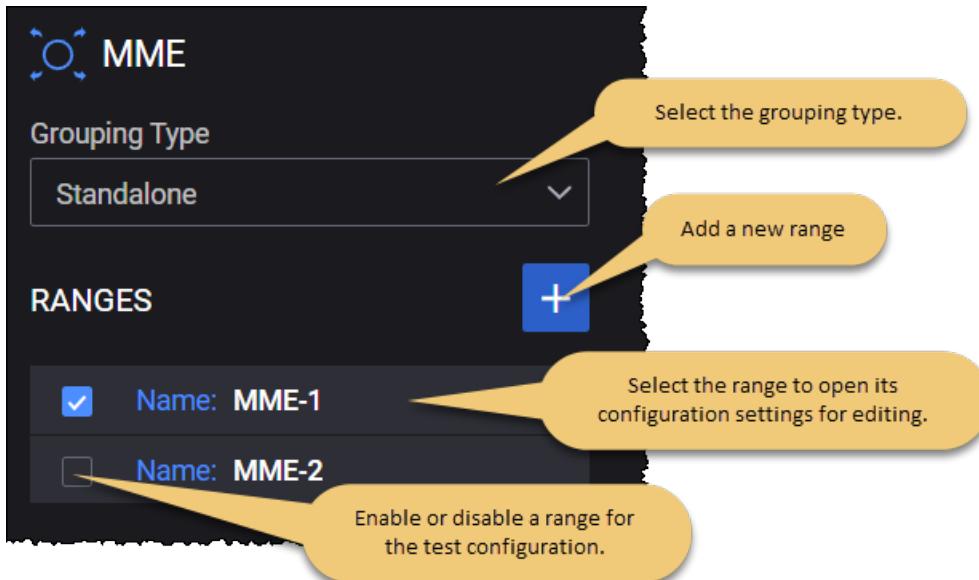
## MME Ranges panel

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

If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All RAN Agents** - This option is available only if **Grouping Type** is set as **With RAN**, and the **N26 Interface** is disabled. Only one MME range grouped with RAN can be configured. This MME range will distribute on all agents by incrementing IP address, etc.
- **Round Robin Ranges on Agents** - This option is available only if the **Grouping Type** is set to **Standalone**, the **N26 Interface** is disabled, and multiple ranges are configured. Each MME Standalone range will require a separate agent.
- **One Range on All Agents** - This option is available only if the **Grouping Type** is set to **Standalone**, and the **N26 Interface** is **disabled**, and only if a single range is configured. Each MME Standalone range will require a separate agent.
- **One Range on One Agent** - This option is available no matter of the **Grouping Type** selection, if the **N26 Interface** is **enabled**, and only if a single range is configured. Each MME Standalone range will require a separate agent.

## 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 <b>Delete Range</b> 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 <a href="#">MME node settings</a> .

<b>Setting</b>	<b>Description</b>
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 <a href="#">MME S11 Interface settings</a> .
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 <a href="#">MME N26 Interface settings</a> .
S1 Interface Settings	These settings are described in <a href="#">MME S1 Interface settings</a> .
S6a Interface Settings	These settings are described in <a href="#">MME S6a Interface settings</a> .
Diameter Settings	These settings are described in <a href="#">MME Diameter settings</a> .

## 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.

<b>Setting</b>	<b>Description</b>
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. <b>About PLMN MCC ...</b> 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.

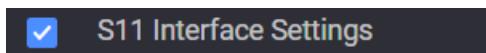
<b>Setting</b>	<b>Description</b>
	The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.
PLMN MNC	<p>The PLMN MNC for this MME range.</p> <p><b>About PLMN MNC ...</b></p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Ciphering Algorithm	<p>The supported 4G ciphering algorithm:</p> <ul style="list-style-type: none"> <li>• EEA0 - Null ciphering algorithm</li> <li>• EEA1 - 128-bit SNOW 3G based algorithm</li> <li>• EEA2 - 128-bit AES based algorithm</li> </ul>
Integrity Algorithm	<p>The supported 4G integrity algorithm:</p> <ul style="list-style-type: none"> <li>• EIA0 - Null Integrity Protection algorithm</li> <li>• EIA1 - 128-bit SNOW 3G based algorithm</li> <li>• EIA2 - 128-bit AES based algorithm</li> </ul>
Relative Capacity	Set the relative capacity value.
Use Full APN	If enabled, the MME uses both APN Network Identifier and Operator Identifier. If disabled, only the APN Network Identifier is used.
Force include ULI in all Modify Bearer Requests	When enabled, will include User Location Information (ULI) IE in all Modify Bearer Request messages sent by MME.
Support for Modify Access Bearers Request Feature	<p><b>IMPORTANT</b> This option appears only if the <b>Grouping Type</b> on the MME node is set to <b>Standalone</b>.</p> <p>In case of Option 3x scenario, it sends the Modify Access Bearers Request message instead of Modify Bearer Request.</p>
T3412	<p><b>IMPORTANT</b> This option appears only if the <b>Grouping Type</b> on the MME node is set to <b>Standalone</b>.</p> <p>Select the check box to enable this option. If enabled, it allows the configuration of the T3412 timer. If disabled, a value of 50 minutes (Value 5 x Unit 10 minutes) is sent for T3412.</p>

Setting	Description
Value	Set the value for this parameter. Accepted values are between <b>0</b> and <b>31</b> .
Unit	Select from the drop-down the unit to use for T3412 timer calculation. Supported values are: <ul style="list-style-type: none"> <li>if <i>Support Extended Timer</i> is <b>enabled</b>, units are <b>2 seconds, 30 seconds, 1 minute, 10 minutes, 1 hour, 10 hours, 320 hours, Deactivated</b>.</li> <li>if <i>Support Extended Timer</i> is <b>disabled</b>, units are <b>2 seconds, 30 seconds, 1 minute, 1 decihour, 10 minutes, 1 hour, 10 hours, Deactivated</b>.</li> </ul>
Support Extended Time	If enabled (default), it sets the T3412 extended value as described in the TS 24301, chapter 8.2.1.12.

## 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.
GTP-C Destination UDP Port	Specify the UDP port that will be used for GTP-C message transmission. Value should be in range of 1024 to 65535.

### Connectivity Settings

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

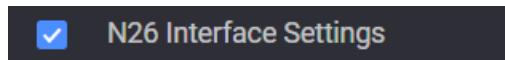
Connectivity setting	Description
IP	Select the IP address to open the IP configuration panel for editing.

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

## 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.
GTP-C Destination UDP Port	Specify the UDP port that will be used for GTP-C message transmission. Value should be in range of 1024 to 65535.

## 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.
<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>

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

## 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:

<b>S1 Interface setting</b>	<b>Description</b>
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

<b>Connectivity setting</b>	<b>Description</b>
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.

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

## 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:



S6a Interface Settings

## Interface Settings

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

<b>Interface setting</b>	<b>Description</b>
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 Transport Port	The local transport port for control plane messages (NG-AP signaling messages). Each SCTP/TCP 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/TCP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP/TCP port.

<b>Interface setting</b>	<b>Description</b>
Remote Transport Port	The remote transport port.
Diameter Transport	Select the diameter transport type: <b>SCTP</b> or <b>TCP</b> .
<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.
<i>SCTP Buffers</i>	
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the SCTP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for SCTP sockets.
<i>TCP Parameters</i>	

Interface setting	Description
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.
Maximum Segment Size (MSS)	The desired Maximum Segment Size (MSS) for the 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).
Use timestamps	Turn on to enable timestamps on TCP packets.
<i>TCP Buffers</i>	
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the TCP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for TCP sockets.

## Connectivity Settings

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

**NOTE**

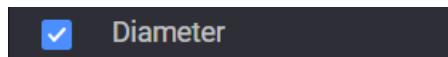
The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity setting	Description
<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).
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
<i>Additional Routes</i>	The additional routes will use the gateway defined in the IP information below.

<b>Connectivity setting</b>	<b>Description</b>
	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.
Gateway Address	The IP address assigned as 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

## 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.

<b>Setting</b>	<b>Description</b>
Origin Host Prefix	Set the origin host prefix. Default value: <b>host</b> .
Origin Realm	Set the origin realm. Default value: <b>keysight.com</b> .

<b>Setting</b>	<b>Description</b>
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:

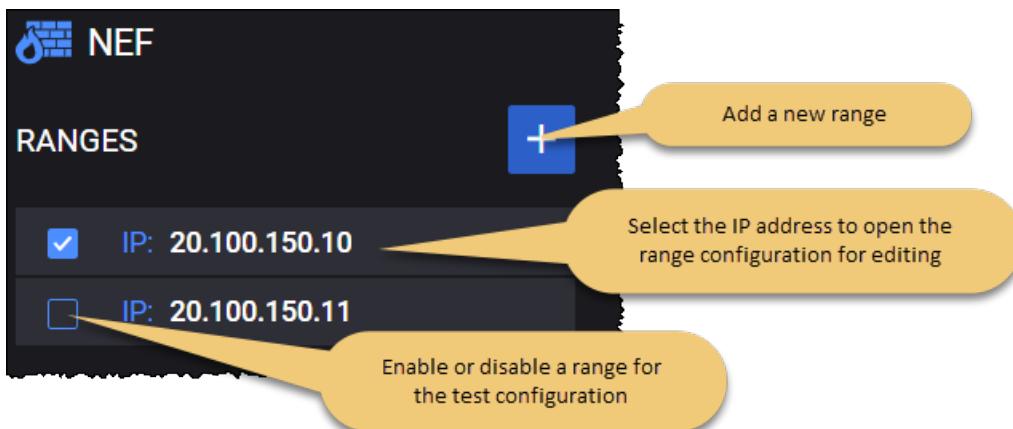
<b>NEF Ranges panel</b>	<b>386</b>
<b>NEF Range panel</b>	<b>387</b>
<b>NEF Node Settings</b>	<b>388</b>
<b>NEF Nnef interface settings</b>	<b>389</b>
<b>NEF Remote SBA Nodes</b>	<b>391</b>
<b>NEF Custom NF Services settings</b>	<b>393</b>

## 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 ...



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents** - Only one NEF Range is supported in a test. The range can be configured on multiple agents. IP addresses and NF IDs will increment on each agent.

## 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 <b>Delete Range</b> 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 (when range is not set as DUT):</i>	
Node Settings	Each AMF range requires the configuration of an associated set of Node Settings, which are described in <a href="#">NEF Node Settings</a> .
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 <a href="#">NEF Nnef interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">NEF Remote SBA Nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nnef IP Address	The IP address from your test network to use for traffic on this interface.
Custom NF Services	This option will allow the configuration of a list of service parameters. See <a href="#">NEF Custom NF Services settings</a> for more information.
TLS Server Name	The name of the server to be sent in SNI extension header in TLS Client Hello message.

## NEF Node Settings

**IMPORTANT** This option appears only if the range is set as DUT.

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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
PLMN MCC	<p>The PLMN MCC for this NEF range.</p> <p><b>About PLMN MCC ...</b></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 NEF range.</p> <p><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
<i>AF ID to ASP ID</i>	
<i>AF ID to ASP ID Map</i>	
	Select the <b>Add AF ID to ASP ID Map</b> button to add a map to your test configuration.
<i>AF ID to ASP ID</i>	
	Select the <b>Delete AF ID to ASP ID</b> button to delete this map from your test configuration.

Setting	Description
AF ID	AF identifier.
ASP ID	ASP identifier.

## NEF Nnef interface settings

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

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

Connectivity Settings	Description
<i>IP</i>	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 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.
Gateway Address	The IP address assigned as gateway address.

<b>Connectivity Settings</b>	<b>Description</b>
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><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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.

The following **Security Settings** enable the necessary Nnfe security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
mTLS Client Settings	Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.
Certificates and Private Keys (.zip )	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</p> <p>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</p>
CA Certificate	Select from the drop-down list one of the available server certificates.
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRTand the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.

Security Settings	Description
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.
	<p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## NEF Remote SBA Nodes

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

## NRF Connection Settings

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

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

Setting	Description
	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"> <li>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.</li> <li>Select <b>Discover</b> to invoke the NF discovery service. Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</li> </ul>
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.

Setting	Description
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.

## NEF Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	

Setting	Description
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the apiRoot for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

# 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:

<b>NRF Ranges panel</b> .....	<b>396</b>
<b>NRF Range panel</b> .....	<b>396</b>
<b>NRF Node settings</b> .....	<b>397</b>
<b>NRF Custom NF Services settings</b> .....	<b>398</b>
<b>NRF Nnrf interface settings</b> .....	<b>399</b>
<b>NRF Remote SBA Nodes</b> .....	<b>401</b>

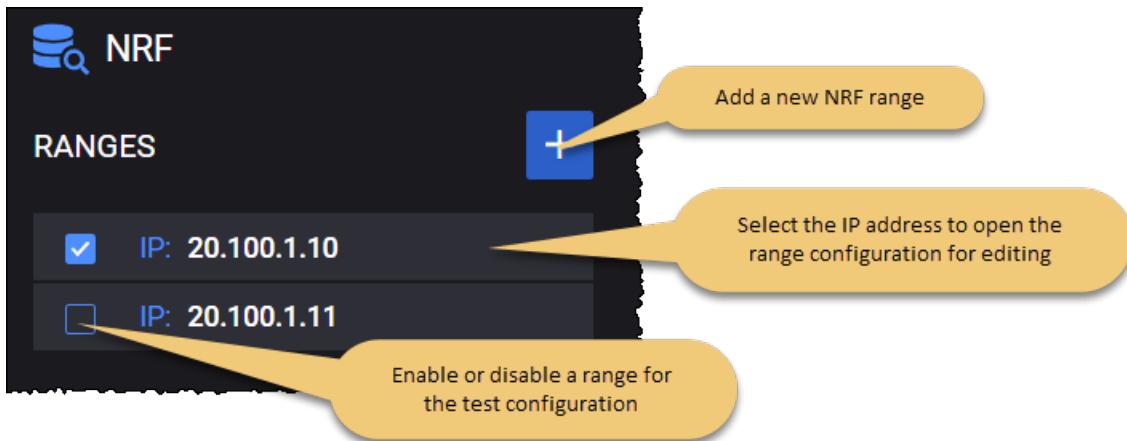
## NRF Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All Ranges on All Agents**
- **Round Robin Ranges on Agents**

## 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
Range:	

Setting	Description
	Select the <b>Delete Range</b> 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 requires the configuration of an associated set of Node Settings, which are described in <a href="#">NRF node settings</a> .
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 <a href="#">NRF Nnrf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">NRF Remote SBA Nodes</a> .
DUT Nnrf IP Address	<b>IMPORTANT</b> This option appears if the range is set as DUT. The IP address from your test network to use for traffic on this interface.
Custom NF Services	<b>IMPORTANT</b> This option appears if the range is set as DUT. This option will allow the configuration of a list of service parameters. See <a href="#">NRF Custom NF Services settings</a> for more information.
TLS Server Name	<b>IMPORTANT</b> This option appears only if the range is set as DUT. The name of the server to be sent in SNI extension header in TLS Client Hello message.

## 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.

Setting	Description
Name	The name of the NRF range. You can accept the name provided by the LoadCore, or you can replace it with a name of your own choosing.
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 Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the apiRoot for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## NRF Nnrf interface settings

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

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

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

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

Connectivity Settings	Description
VLAN ID	VLAN identifier.
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

The following **Security Settings** enable the necessary Nnrf security interaction.

Security Settings	Description
<i>TLS Settings</i>	
mTLS Client Settings	Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</p>
CA Certificate	Select from the drop-down list one of the available server certificates.
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p>

<b>Security Settings</b>	<b>Description</b>
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	<p>Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.</p>
Active Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.</p>
Staged Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.</p> <p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## NRF Remote SBA Nodes

### Remote SEPP

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

<b>Setting</b>	<b>Description</b>
Peer SEPP	<p>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.</p>
Protocol	<p>The protocol to use for communication via SCP. It can be either HTTP or HTTPS.</p>
Port	<p>The port number to use for communication via SCP. The default is port 80, but you can choose a different port number.</p>

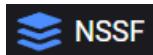
Setting	Description
Sepp Communication Type	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Telescopic FQDN</b></li> <li>• <b>Target API Root</b></li> </ul>
Force FQDN Mapping	Select this option to enable it.

## Remote NRFs

The following configuration settings are required.

Setting	Description
<i>Remote NRFs :</i>	
	Select the <b>Add Remote NRF</b> button to add a new remote NRF to your test configuration.
<i>Remote NRF:</i>	
	Select the <b>Delete Remote NRF</b> button to delete the remote NRF range from your test configuration.
Peer NRF	Select the IP address of the peer NRF.
FQDN	The value has the following form: <code>&lt;instanceID&gt;.5gc.mnc&lt;value1&gt;.mcc&lt;value2&gt;.3gppnetwork.org:</code> <ul style="list-style-type: none"> <li>• <code>instanceID</code> of the selected remote NRF</li> <li>• <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)</li> <li>• <code>value2</code> is the PLMN MCC of the selected remote NRF</li> </ul>
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:

<b>NSSF Ranges panel</b>	<b>404</b>
<b>NSSF Range panel</b>	<b>404</b>
<b>NSSF Node settings</b>	<b>405</b>
<b>Nnssf Interface Settings</b>	<b>406</b>
<b>Remote SBA nodes</b>	<b>409</b>
<b>NSSF Restricted NSSAIs</b>	<b>409</b>
<b>NSSF Network Slices</b>	<b>411</b>
<b>NSSF Configured NSSAI</b>	<b>412</b>

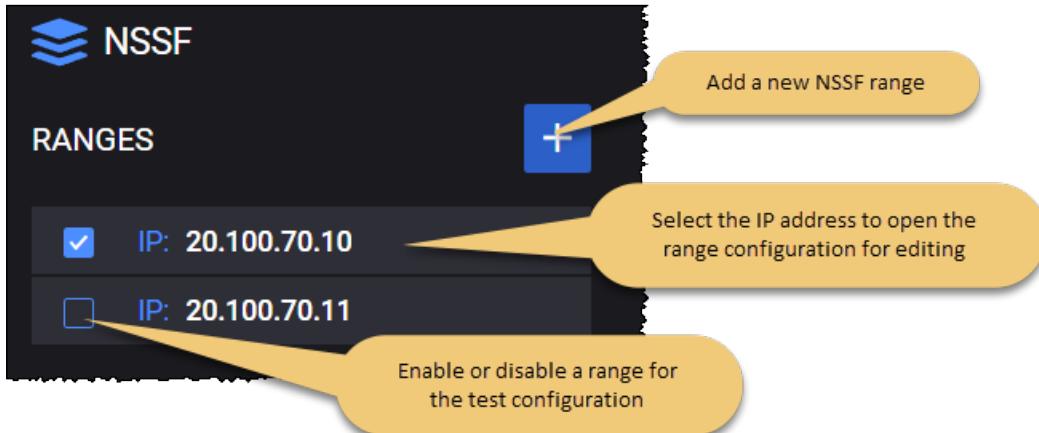
## NSSF Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT** Only one NSSF Range can be configured on one agent.

- in case of multiple ranges it will require one agent for each range;
- in case of one range and multiple agents, each agent will create a different NSSF NF, with incremented IP address and NF ID, and a whole UE range.

## 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 <b>Delete Range</b> 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 (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 <a href="#">NSSF node settings</a> .
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 <a href="#">Nnssf Interface Settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">Remote SBA nodes</a> .
<i>Network Slicing:</i>	
Restricted NSSAIs	These settings are described in <a href="#">NSSF Restricted NSSAIs</a> .
Network Slices	These settings are described in <a href="#">NSSF Network Slices</a> .
Configured NSSAIs	These settings are described in <a href="#">NSSF Configured NSSAI</a> .

## NSSF Node settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple NSSF instances may be deployed in the 5G network. Each NSSF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.

Setting	Description
PLMN MCC	<p>Set the mobile country code.</p> <p><b>About PLMN MCC ...</b></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>Set the mobile network code.</p> <p><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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

Connectivity Setting	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.
<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.

The following **Security Settings** enable the necessary Nnssf security interaction.

Security Settings	Description
<i>TLS Settings</i>	
<i>mTLS Client Settings</i>	Select the check-box to make this option available, and then select the <i>mTLS Client Settings</i> to open the configuration panel for editing.
Certificates and Private Keys (.zip )	You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.
	<b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.

<b>Security Settings</b>	<b>Description</b>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
CA Certificate	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	<p>Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.</p>
Active Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.</p>
Staged Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.</p>

Security Settings	Description
	<p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## Remote SBA nodes

### NRF Connection Settings

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

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

### SCP Connection Settings

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

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

## NSSF Restricted NSSAIs

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

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

<b>Setting</b>	<b>Description</b>
<i>Restricted NSSAIs:</i>	
	Select the <b>Add a restricted NSSAI</b> button to add a restricted NSSAI to your test configuration.
<i>Restricted NSSAI settings:</i>	
	Select the <b>Delete Restricted NSSAI</b> 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 <b>Add NSSAI</b> button to add a Restricted A-NSSAI to your test configuration.
<i>NSSAI Settings:</i>	
	Select the <b>Delete NSSAI</b> button to delete this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The default Mapped configure Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The default Mapped configured Slice Differentiator (SD) value for this S-NSSAI.

## NSSF Network Slices

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

Setting	Description
<i>Network Slices:</i>	
	Select the <b>Add a Network slice</b> button to add a network slice to your test configuration.
<i>Network Slice settings:</i>	
	Select the <b>Delete a Network Slice</b> 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 <b>Add Tracking Area</b> button to add a Tracking Area (TA) to your test configuration.
<i>Tracking Area Indication (TAI) settings:</i>	
	Select the <b>Delete TAI</b> 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 <b>Add a Configured NSSAI</b> button to add a Configured NSSAI to your test configuration.
<i>Configured SNSSAI settings:</i>	
	Select the <b>Delete a Configured NSSAI</b> 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 <b>NSSF Network Slices</b> 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:

<b>PCF/PCRF Ranges panel</b>	<b>414</b>
<b>PCF Range panel</b>	<b>415</b>
<b>PCF Node settings</b>	<b>416</b>
<b>PCF Custom NF Services settings</b>	<b>418</b>
<b>PCRF Node settings</b>	<b>418</b>
<b>PCF service area restrictions</b>	<b>421</b>
<b>PCF Npcf interface settings</b>	<b>423</b>
<b>PCF remote SBA nodes</b>	<b>424</b>

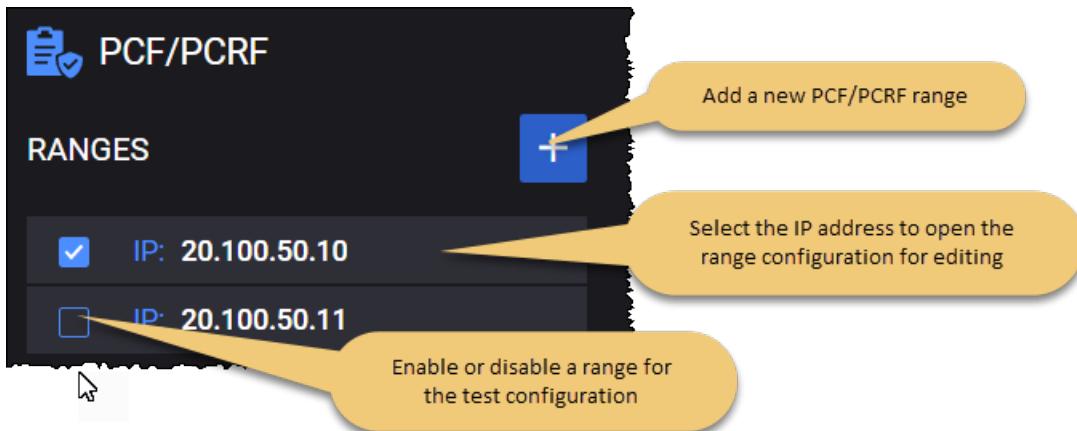
## PCF/PCRF Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT** Only one PCF range can be configured on one agent:

- in case of multiple ranges, it will require one agent for each range.
- in case one range and multiple agents, each agent will create a different PCF NF, with incremented IP address and NF ID, and whole UE range.

## 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 <b>Delete Range</b> 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>	
RAT Type	This option allows you to enable only the functionalities specific to the selected Radio Access Technology type (RAT). Options available are: <b>5G</b> , <b>4G</b> , or <b>5G and 4G</b> .  <b>NOTE</b> Only the 4G option supports Gx Interface for 4G Stand Alone Core Network. The other options use the Dual Core Network which uses SBA interface between SMF/(S)PGW-C and PCF.
Node Settings	Each PCF range the configuration of an associated set of Node Settings, which are described in <a href="#">PCF node settings</a> .
Custom NF Services	<b>IMPORTANT</b> This option appears if the range is set as DUT.  This option will allow the configuration of a list of service parameters. See <a href="#">AMF Custom NF Services settings</a> for more information.
PCRF Node Settings	These settings are described in <a href="#">PCRF node settings</a> .
Service Area Restrictions	Each PCF range requires the configuration of the service area restrictions. The settings are described in <a href="#">PCF service area restrictions</a> .
Npcf	Each PCF range requires the configuration of Npcf interface settings, through

Setting	Description
Interface Settings	which a PCF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in <a href="#">PCF Npcf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">PCF remote SBA nodes</a> .
TLS Server Name	<p><b>IMPORTANT</b> This option appears only if the range is set as DUT.</p> <p>The name of the server to be sent in SNI extension header in TLS Client Hello message.</p>

**NOTE**

In case of [Home-Routed](#) roaming there are two PCF nodes involved, one in visited PLMN and one in home PLMN. The LoadCore agent allows only one PCF node configuration, thus when multiple PCF nodes are configured in LoadCoreUI, multiple [agents](#) need to be configured as well with a 1:1 ratio.

## PCF Node settings

Each PCF range includes a set of Node Settings.

### Node Settings

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

Setting	Description
Instance ID	<p>Multiple PCF instances may be deployed in the 5G network.</p> <p>Each PCF instance is uniquely identified by an <i>Instance ID</i>. You can accept the value provided by LoadCore or overwrite it with your own value.</p>
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
Name	The name of the PCF range. You can accept the name provided by the LoadCore, or you can replace it with a name of your own choosing.
PLMN MCC	<p>The PLMN MCC for this PCF range.</p> <p><b>About PLMN MCC ...</b></p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this PCF range.</p> <p><b>About PLMN MNC ...</b></p>

<b>Setting</b>	<b>Description</b>
	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.
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.
Retrieve Operator Specific Data	Retrieve Operator Specific Data from UDR during SM Policy Establishment.
Triggers	<p>Request Triggers to which the PCF subscribes. The allowed values are:</p> <ul style="list-style-type: none"> <li>• Location Change (tracking area). The tracking area of the UE has changed.</li> <li>• PRA Change (change of UE presence in PRA). The UE is entering/leaving a Presence Reporting Area.</li> </ul> <p>Both values can be selected simultaneously.</p>
Ask Result Notification from SMF for Create/Delete QoS Flow	If needed, enable this option.
Retrieve AM Policy Data	If enabled, the PCF will retrieve AM Policy data from UDR.
RAT Type Awareness	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Ignore</b></li> <li>• <b>5G Only</b></li> <li>• <b>4G Only</b></li> </ul>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## PCF Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## PCRF Node settings

The following settings are required to configure the PCRF node.

Settings	Description
Rx Interface Settings	Select the check-box to enable this option, and then open the <a href="#">Rx Interface Settings</a> panel for editing.
Gx Interface Settings	<b>IMPORTANT</b> This menu is available only if <b>RAT Type</b> value under <a href="#">PCF Range panel</a> is set to <b>4G</b> . Select to open the <a href="#">Gx Interface Settings</a> panel for editing.

## Rx/Gx Interface Settings

The following settings are available to configure the Rx/Gx Interface.

Settings	Description
Diameter	Select to open the Diameter settings panel.

<b>Settings</b>	<b>Description</b>
<i>Settings</i>	
Origin Host Prefix	Set the origin host prefix. Default value: <b>host</b> .
Origin Realm	Set the origin realm. Default value: <b>keysight.com</b> .
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.
<i>SCTP Parameters</i>	<i>Select to open the configuration panel.</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.
<i>SCTP Buffers</i>	<i>Select to open the configuration panel.</i>
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the SCTP sockets.

Settings	Description
Rx Buffers (bytes)	The size (in bytes) of receive buffers for SCTP sockets.
<i>TCP Parameters</i>	<i>Select to open the configuration panel.</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.
Maximum Segment Size (MSS)	<p>The desired Maximum Segment Size (MSS) for the 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>
Use timestamps	Turn on to enable timestamps on TCP packets.
<i>TCP Buffers</i>	<i>Select to open the configuration panel.</i>
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the TCP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for TCP sockets.
<i>Connectivity Settings</i>	
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address 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).
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
<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.

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

## 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.

<b>Setting</b>	<b>Description</b>
<i>Service Area Restrictions:</i>	
Restriction type	<p>Set the restriction type attribute:</p> <ul style="list-style-type: none"> <li>• Allowed Areas</li> <li>• Not Allowed Areas</li> </ul>
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 <b>Add Area</b> button to add a new restriction area to your configuration.
<i>Area:</i>	
	Select the <b>Delete Area</b> 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 <b>Add TAC</b> 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 <b>Delete</b> 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>	<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.
Gateway Address	The IP address assigned as 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the IP's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</p>
CA Certificate	Select from the drop-down list one of the available server certificates.
Certificates and Private Keys (.zip)	You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.
mTLS Client Settings	Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.
Certificates and Private Keys (.zip )	You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.

## 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 Connection Settings:</i>	
Peer UDR	<p>Select the peer UDR using either of the following methods:</p> <ul style="list-style-type: none"> <li>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.</li> <li>Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>
Protocol	The protocol to use for Nudr communications. It can be either HTTP or HTTPS.
Port	The UDR port number to use for Nudr communications. The default is port 80, but you can choose a different port number.

## NRF Connection Settings

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

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

## DNS Server Connection Settings

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.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

# 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.

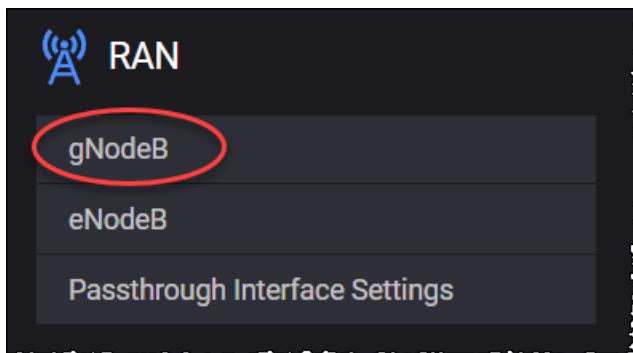
The configuration settings are described in the topics listed below.

## Topics:

<b>gNodeB</b>	<b>427</b>
gNodeB Ranges panel	428
gNodeB Range settings	433
gNodeB Node settings	434
gNodeB NSSAI settings	436
gNodeB N2 interface settings	437
gNodeB N3 interface settings	440
<b>eNodeB</b>	<b>442</b>
eNodeB Ranges panel	443
eNodeB Range Settings	447
eNodeB Node Settings	447
S1-U Interface Settings	449
S1-MME Interface Settings	450
<b>Passthrough interface settings</b>	<b>453</b>

## 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:

<b>gNodeB Ranges panel</b> .....	<b>428</b>
<b>gNodeB Range settings</b> .....	<b>433</b>
<b>gNodeB Node settings</b> .....	<b>434</b>
<b>gNodeB NSSAI settings</b> .....	<b>436</b>
<b>gNodeB N2 interface settings</b> .....	<b>437</b>
<b>gNodeB N3 interface settings</b> .....	<b>440</b>

## gNodeB Ranges panel

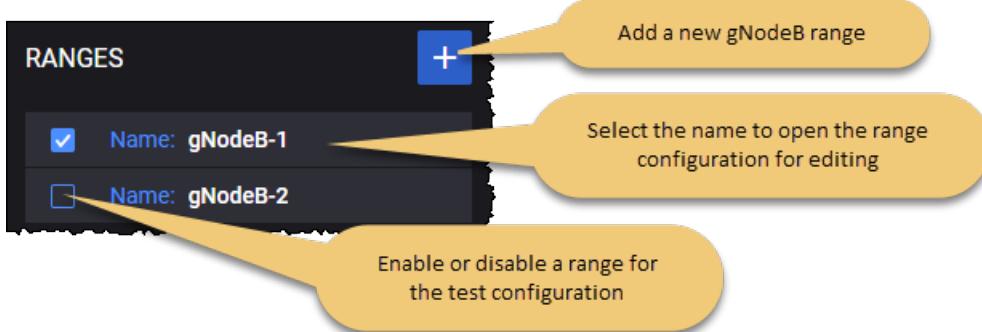
The **gNodeB Ranges** panel opens when you select **gNodeB** from the RAN pane. It consists of two main section: Ranges and Ranges Connectivity.

### Ranges

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

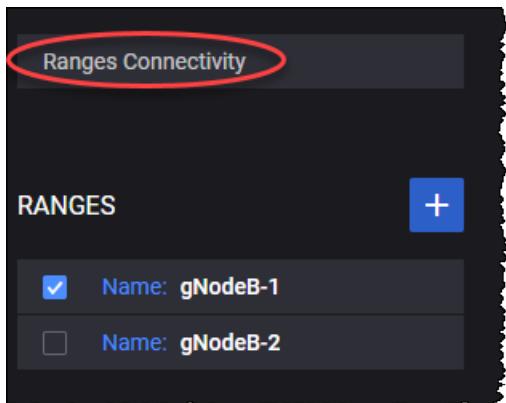
- Add a new gNodeB range to your test configuration.
- Open a gNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

#### For example ...



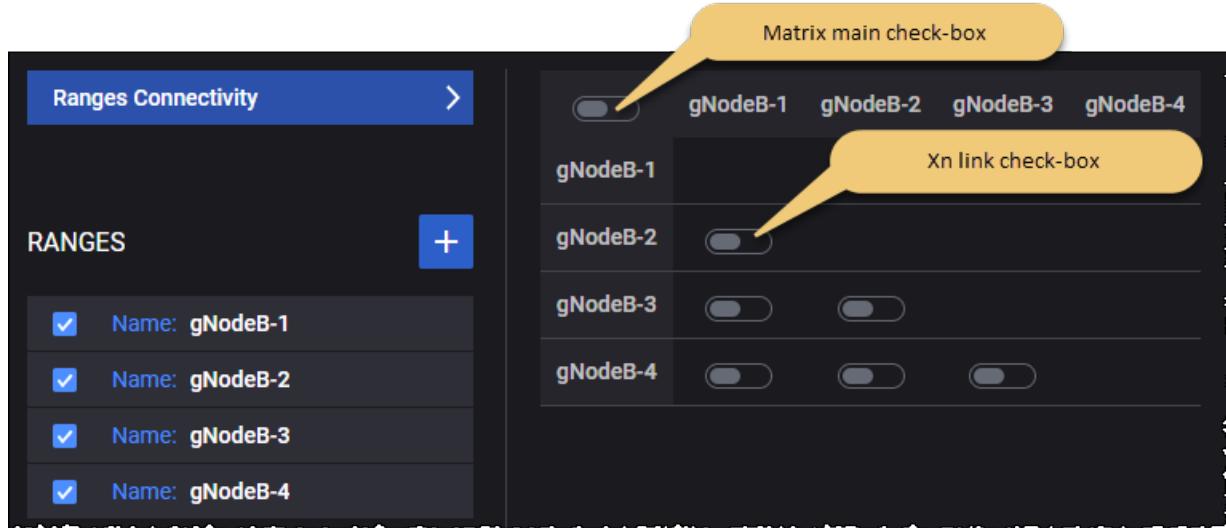
### Ranges Connectivity

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.

The screenshot shows the 'Ranges Connectivity' configuration screen. On the left, under 'RANGES', there is a list of gNodeB ranges: gNodeB-1, gNodeB-2, gNodeB-3, gNodeB-4 (disabled), gNodeB-5, and gNodeB-6. The 'gNodeB-4' range is circled in red. On the right, a grid shows connections between these ranges. The columns are labeled gNodeB-1, gNodeB-2, gNodeB-3, gNodeB-4, gNodeB-5, and gNodeB-6. The rows are also labeled with these names. A red box highlights the row for 'gNodeB-4'. Red arrows point from the circled 'gNodeB-4' in the list to the highlighted row in the grid, and from the highlighted row in the grid to the 'gNodeB-4' row in the list.

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.

This screenshot shows the same 'Ranges Connectivity' interface after some changes. The 'RANGES' list now includes gNodeB-1, gNodeB-2, gNodeB-3, gNodeB-4 (disabled), gNodeB-5 (enabled), and gNodeB-6. The 'gNodeB-4' range is circled in red. In the grid, the connection between gNodeB-3 and gNodeB-4 is now greyed out (indicated by a greyed-out checkmark). The connection between gNodeB-3 and gNodeB-6 is also greyed out. The 'gNodeB-5' and 'gNodeB-6' rows in the grid have blue checkmarks in their first two columns, while the last four columns are greyed out.

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.

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

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

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

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

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

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

## gNodeB Range settings

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

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

## gNodeB range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the <b>Delete Range</b> 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 <a href="#">gNodeB node settings</a> .
NSSAI	Each gNodeB range requires the configuration of at least one NSSAI, and may specify multiple NSSAIs. These settings are described in <a href="#">gNodeB NSSAI settings</a> .
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 <a href="#">gNodeB N2 interface settings</a> .
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 <a href="#">gNodeB N3 interface settings</a> .

## 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.
Dynamic RAN UE NGAP/S1AP ID	If enabled, it will allocate dynamic RAN UE NGAP/S1AP ID values at Service Request.

### EPS Fallback Settings

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

The following parameters are required to configure the EPS fallback:

Setting	Description
Enable EPS Fallback	Select the check box to enable this option.
5QI	Select the 5G QoS identifier that will trigger the EPS fallback procedure. (The 5QI must be defined on the <a href="#">QoS Flow configuration settings on page 138</a> panel in the <b>Global Settings</b> .) When a request is received for this 5QI to create a dedicated QoS flow, the RAN will reject the request, which will trigger the EPS fallback procedure.
Associated ENB	Select the eNodeB used for handover.
Secondary Node	Select the secondary node from the drop-down list. This option is used for EPS fallback to an eNodeB associated to a gNodeB using Option 3x.
EPS Fallback Mobility	Type of mobility to EPS during EPS fallback. Select an option from the drop down list: <ul style="list-style-type: none"> <li>• <b>Handover to 4G</b></li> <li>• <b>Inter-System Redirection to 4G</b></li> </ul>
EPS Fallback Return Mobility	Type of mobility that occurs after the deletion of the dedicated bearer that triggered EPS fallback. Select an option from the drop down list: <ul style="list-style-type: none"> <li>• <b>None</b> - After the dedicated bearer is deleted in 4G, the UE will not initiate any procedure.</li> <li>• <b>Connected Mode Handover to 5G</b> (default value) - After the dedicated bearer is deleted in 4G, the UE will initiate a 4G to 5G Connected Mode Handover.</li> <li>• <b>Idle Mode Mobility to 5G</b> - 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.</li> </ul>
Send Service Request After EPS Fallback Return Mobility	By default, this option is disabled. Send Service Request immediately after returning to 5G when Idle Mode Mobility to 5G was performed.

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

**NOTE**

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

## gNodeB NSSAI settings

Each UE range requires at least one NSSAI range.

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

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

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

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

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

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

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

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

<b>Setting</b>	<b>Description</b>														
SST	The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are:														
	<table border="1"> <thead> <tr> <th><b>SST</b></th> <th><b>Value</b></th> <th><b>Suitable for handling:</b></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>			<b>SST</b>	<b>Value</b>	<b>Suitable for handling:</b>	eMBB	1	5G enhanced Mobile Broadband	URLCC	2	ultra-reliable low-latency communications	MIoT	3	massive IoT
<b>SST</b>	<b>Value</b>	<b>Suitable for handling:</b>													
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

<b>Settings</b>	<b>Description</b>
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

<b>Settings</b>	<b>Description</b>
	addresses through which that endpoint can be reached and from which it will originate SCTP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP port. The default port number is 36412, but you can change it.
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum 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.
SCTP Retry	<i>Select the check box to enable this option.</i>
Delay	<p>The delay time (in milliseconds) for triggering a new SCTP retry, after a SCTP disconnect or a failed retry. For subsequent SCTP retries, consider the Connection Timeout value that will be added as well.</p> <p>Default value: <b>0</b>. Allowed integer value: minimum of 0.</p>
Number of Retries	<p>The maximum number of SCTP retries sent by RAN to reestablish the SCTP connection.</p> <p>Default value: <b>3</b>. Allowed integer value: minimum of 1.</p>

## Connectivity Settings

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).
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>	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	<b>IMPORTANT</b> This option is visible only when the Outer VLAN 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.

Settings	Description
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.

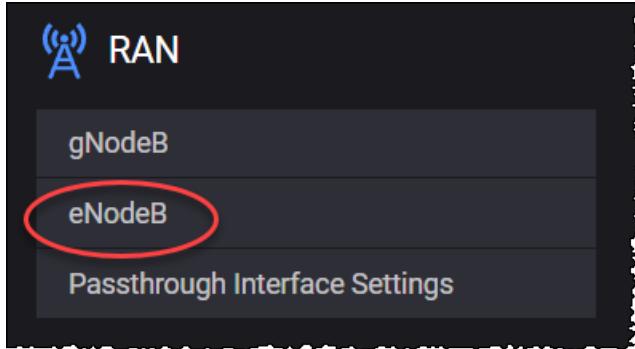
**NOTE** The following connectivity settings are available in LoadCore WebUI, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
<i>IP</i>	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).
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. <b>NOTE</b> 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>	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	<b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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..

## 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:

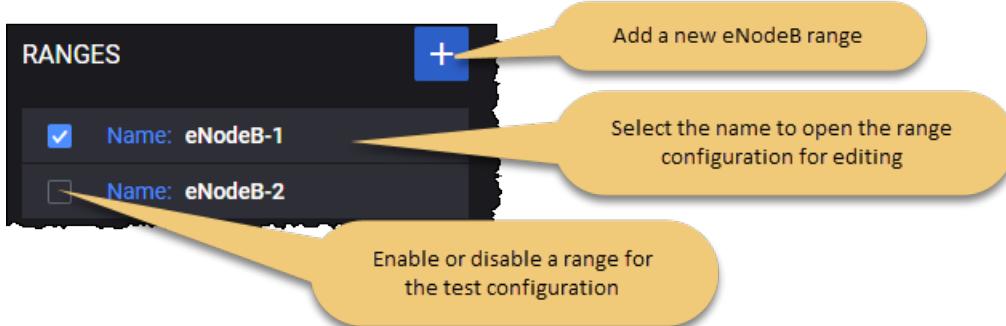
<b>eNodeB Ranges panel</b> .....	<b>443</b>
<b>eNodeB Range Settings</b> .....	<b>447</b>
<b>eNodeB Node Settings</b> .....	<b>447</b>
<b>S1-U Interface Settings</b> .....	<b>449</b>
<b>S1-MME Interface Settings</b> .....	<b>450</b>

## 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:

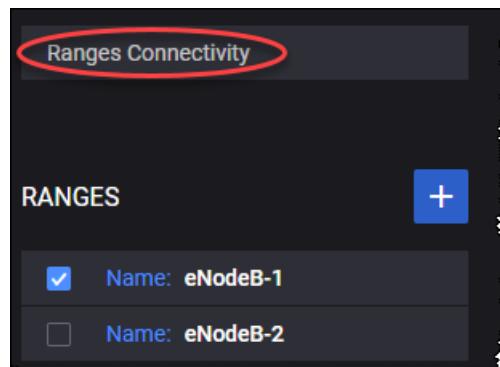
- Add a new eNodeB range to your test configuration.
- Open a eNodeB range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



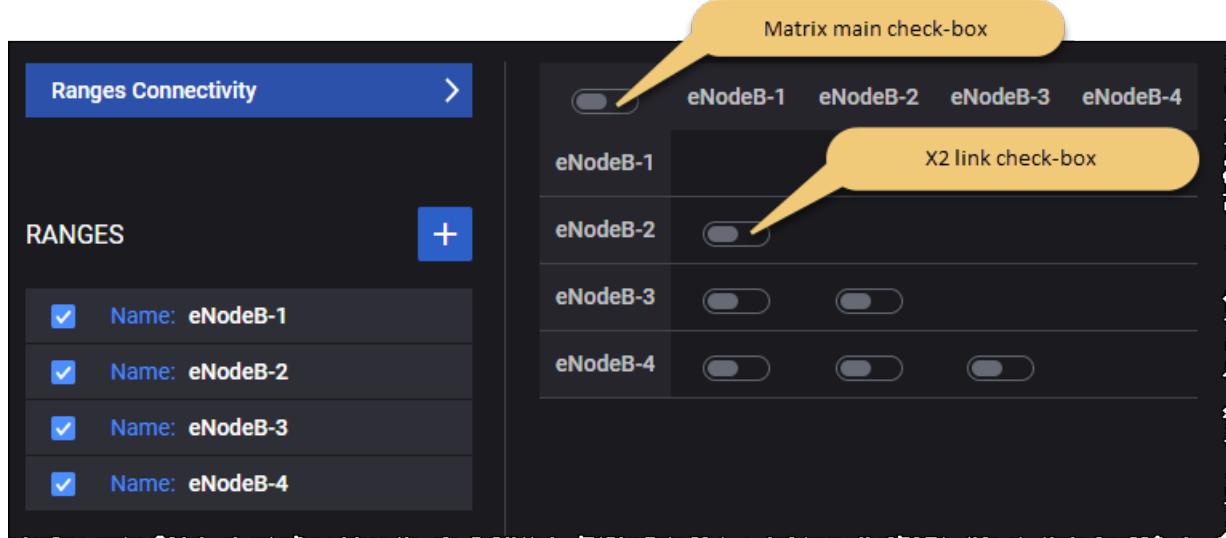
## Ranges Connectivity

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:

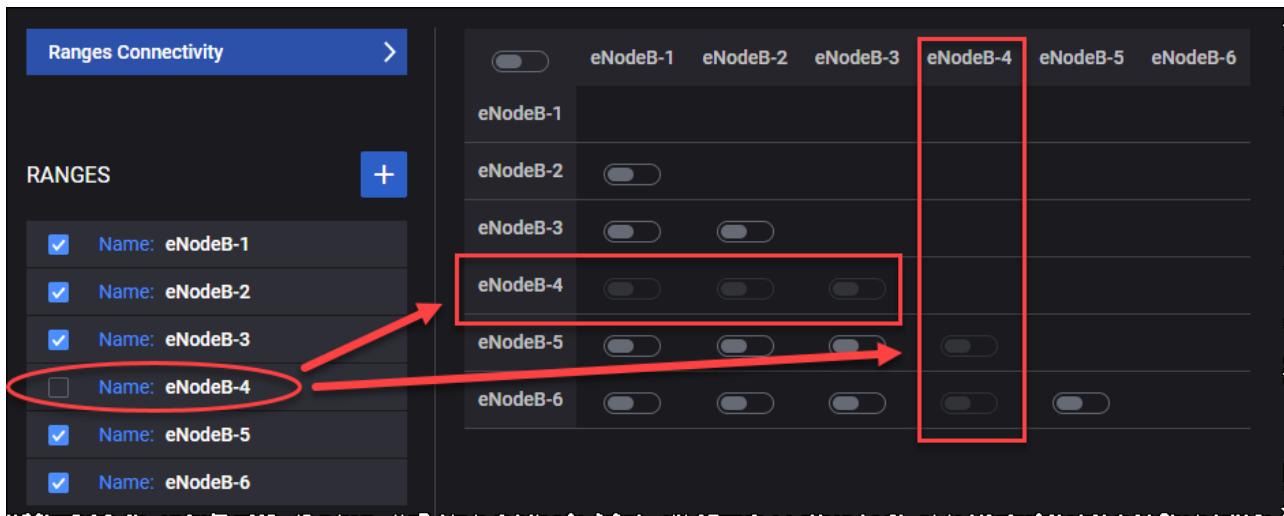
State	Description
Selected and blue color	An X2 link connection is established between enabled eNodeB ranges.
Selected and grey color	An X2 link connection is established between disabled eNodeB ranges.
Unselected	No X2 link connection between eNodeB ranges.

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.

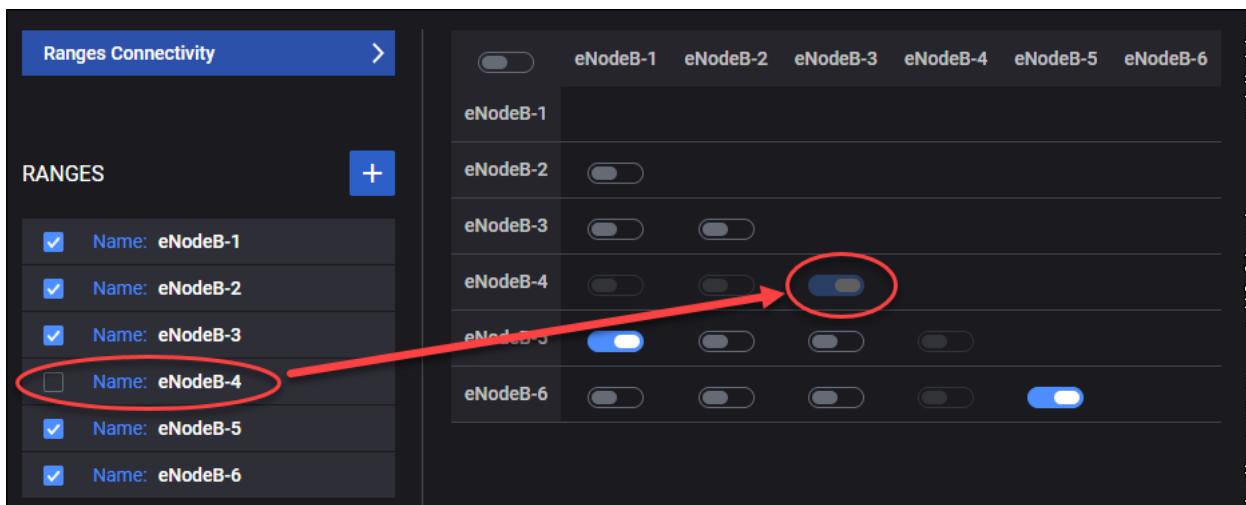


If there was an X2 link between two eNodeB ranges and now one of them is disabled, the check-box will become greyed out and cannot be unselected.

**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 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: 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 7x7 matrix of checkboxes representing X2 links between eNodeBs. The columns and rows are labeled eNodeB-1 through eNodeB-7. The first cell in the top-left corner contains a main checkbox that is checked. All other individual checkboxes in the matrix are also checked.

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, showing the 'Ranges Connectivity' interface. The list of ranges and their checkboxes remain the same. The matrix of X2 link checkboxes is identical, with all individual checkboxes being checked. The main matrix checkbox at the top-left is highlighted with a red circle.

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 <b>Delete Range</b> button to delete this range from your test configuration.
<i>Range Count</i>	
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 <a href="#">eNodeB node settings</a> .
S1-U Interface Settings	Each eNodeB range requires the configuration of an associated set of S1-U Interface Settings, which are described in <a href="#">S1-U interface settings</a> .
S1 Interface Settings	Each eNodeB range requires the configuration of an associated set of S1 Interface Settings, which are described in <a href="#">S1-MME interface settings</a> .

## 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

Setting	Description
	eNodeB ID 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.
Dynamic RAN UE NGAP/S1AP ID	If enabled, it will allocate dynamic RAN UE NGAP/S1AP ID values at Service Request.

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

Setting	Description
Public Warning System	Select the check box to enable this option.
PWS Restart Timer (s)	Duration in seconds after which PWS Restart Indication is sent. The timer starts after the PWS Write-Replace message exchange. <b>0</b> indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.3 PWS Restart Indication</i> . Values should be in range 0-86400. Default value: <b>0</b> .
PWS Failure Timer (s)	Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. <b>0</b> indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.4 PWS Failure Indication</i> . Values should be in range 0-86400. Default value: <b>0</b> .

**NOTE**

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

## S1-U Interface Settings

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

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

### Connectivity Settings

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

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

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

## 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-MME 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.
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum	Set the maximum retransmission timeout value, in milliseconds.

S1-MME Interface Settings	Description
Retransmission Timeout (ms)	
Initial Retransmission Timeout (ms)	Set the initial retransmission timeout value, in milliseconds.
Maximum Retransmission per Association	Set the maximum retransmissions value per association.
Maximum Retransmission per Path	Set the maximum retransmissions value per path.
Heartbeat Interval (ms)	Set the heartbeat interval value, in milliseconds.
SACK Delay (ms)	Set the delayed selective ACK timeout value.
SACK Frequency	Set the delayed selective ACK frequency value.
SCTP Retry	<i>Select the check box to enable this option.</i>
Delay	The delay time (in milliseconds) for triggering a new SCTP retry, after a SCTP disconnect or a failed retry. For subsequent SCTP retries, consider the Connection Timeout value that will be added as well. Default value: <b>0</b> . Allowed integer value: minimum of 0.
Number of Retries	The maximum number of SCTP retries sent by RAN to reestablish the SCTP connection. Default value: <b>3</b> . Allowed integer value: minimum of 1.

## Connectivity Settings

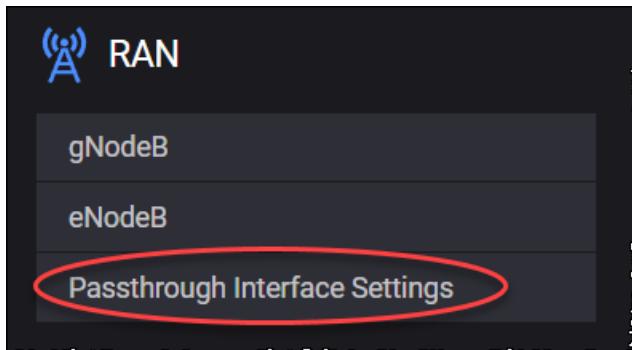
The following table describes the parameters that you need to configure for the connectivity settings:

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

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

## 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	<b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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:

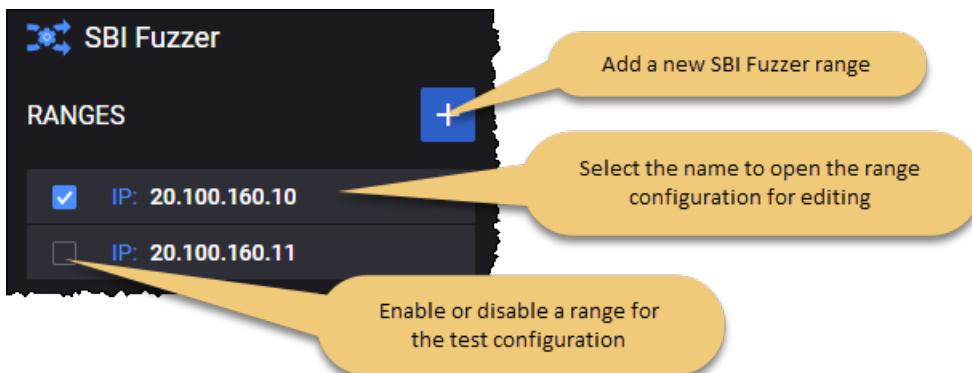
<b>SBI Fuzzer Ranges panel</b>	<b>455</b>
<b>SBI Fuzzer Range panel</b>	<b>456</b>
<b>SBI Node Settings</b>	<b>457</b>
<b>SBI Fuzzer interface settings</b>	<b>459</b>
<b>SBI Fuzzer Target Node</b>	<b>461</b>

## 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 ...



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**
- **All Ranges on One Agent**

### IMPORTANT

Distribution modes change based on the number of ranges and agents configured on this node.

## 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 <b>Delete Range</b> 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 <a href="#">SBI Fuzzer node settings</a> .
Interface Settings	These settings are described in <a href="#">SBI Fuzzer interface settings</a> .
Target Nodes	The target node settings are described in <a href="#">SBI Fuzzer target nodes</a> .
<b>NOTE</b>	Although <code>content-type: multipart/related</code> may contain JSON parts, this type of message will not be fuzzed.
<b>NOTE</b>	SBI Fuzzer cannot be used in combination with SCP or SEPP.
<b>NOTE</b>	Messages with <code>content-type: application/problem+json</code> will not be modified.
<b>NOTE</b>	Impairment script cannot be applied to the agent on which SBI Fuzzer runs on.

## SBI 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"> <li>• <b>Requests Only</b></li> <li>• <b>Responses Only</b></li> <li>• <b>Requests and Responses</b></li> </ul>
Fuzzing Algorithm	Select the fuzzing algorithm type from the drop-down list. Available options: <ul style="list-style-type: none"> <li>• <b>Forward Unchanged</b> - does not modify the original body.</li> <li>• <b>Duplicated JSON Entries</b> - duplicates a random key-value pair from the original body.</li> <li>• <b>Extra JSON Values</b> - adds extra key-value pairs that are generated randomly to the original body.</li> <li>• <b>Extra Spaces</b> - adds extra spaces.</li> <li>• <b>Integer Overflow</b> - modifies integer value to an overflow value.</li> <li>• <b>Duplicated JSON Entries With Wrong Values</b> - duplicates a random key from the original body and modifies its value to a random string.</li> <li>• <b>Custom Fuzzing Script</b> - uses a custom impairment script.</li> </ul>
Use Random Values for Fuzzing Algorithms	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Duplicated JSON Entries, Extra JSON Values, Extra Spaces, Integer Overflow</b> or <b>Duplicated JSON Entries with Wrong Values</b> . If enabled, it will use random values for fuzzing algorithms.
IE Index to be duplicated	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Duplicated JSON Values</b> . Identifies the <i>key:value</i> pair to be duplicated. Use 0 to identify the first key in the JSON body. The added item will be placed at the end of the JSON body.
Extra Values Pairs	<i>This option appears only if Fuzzing Algorithm is set as Extra JSON Values.</i> <i>Select this option to open the configuration panel (see <a href="#">Extra Values Pairs</a>).</i>
Pad Extra Spaces to String IE	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Extra Spaces</b> . If selected, it will pad with spaces the string value of the selected <i>key:value</i> pair. If not selected, it will add spaces at the end of the JSON body.
String IE Index to be	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Extra Spaces</b> , and <b>Pad Extra Spaces to String IE</b> is enabled.

Setting	Description
Padded	The string to be padded.
Number of Spaces to Pad	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Extra Spaces</b> . The number of <space> characters to be added.
Integer IE Index to Modify	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Integer Overflow</b> . Identifies the Integer to be modified in JSON body. To modify first integer value, use 0.
New Integer IE Value	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Integer Overflow</b> . The new integer value in any of the following formats: 0xffffffff, 1.79769313486e+308, -1.79769313486e+308, 1664914247222295162770764775.
IE Index to be duplicated (Wrong Value)	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Duplicated JSON Entries with Wrong Values</b> . Identifies the <i>key:value</i> pair to be duplicated. Use 0 to identify the first key in JSON body. The added item will be placed at the end of the JSON body.
New IE Value	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Duplicated JSON Entries with Wrong Values</b> . The new string value for this key.
Custom Fuzzing Script	This option appears only if <b>Fuzzing Algorithm</b> is set as <b>Custom Fuzzing Script</b> . Use the <b>Upload</b> button to load a custom impairment script. Use <b>Clear</b> to remove it.  <b>IMPORTANT</b> At SBI Fuzzer range level, Custom Fuzzing scripts are uploaded and assigned per SBI Fuzzer range. But, at a global level, scripts can be imported, exported and deleted from <a href="#">Settings &gt; Library &gt; Resource Library &gt; Custom Fuzzing Scripts</a> .

**NOTE** Although `content-type: multipart/related` may contain JSON parts, this type of message will fuzz the first JSON part of a multipart message.

**NOTE** SBI Fuzzer cannot be used in combination with SCP or SEPP.

**NOTE** Messages with `content-type: application/problem+json` will not be modified.

**NOTE** Impairment script cannot be applied to the agent on which SBI Fuzzer runs on.

## Extra Values Pairs

Setting	Description
<i>Extra Values Pairs</i>	
	Select the Add button to add an extra pair of values to your test configuration.
<i>Extra Values Pair</i>	
	Select the Delete button to delete the extra pair of values from your test configuration.
Key	The string value for the KEY in a new <i>key:value</i> pair, to be added to the JSON body.
Value	The string value of a <i>key:value</i> pair to be added to the JSON body

## 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.
<i>Additional Routes</i>	<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.

<b>Connectivity Settings</b>	<b>Description</b>
	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.
Gateway Address	The IP address assigned as 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.

The following **Security Settings** enable the necessary SBI Fuzzer security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
mTLS Client Settings	<i>Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.</i>
Certificates and Private Keys (.zip )	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
CA Certificate	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>

<b>Security Settings</b>	<b>Description</b>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate.</p> <p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## SBI Fuzzer Target Node

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

<b>Setting</b>	<b>Description</b>
SBA Peer	Select the peer node from the drop-down list. Available options: <b>None</b> (default value), <b>NRF</b> , <b>AUSF</b> , <b>PCF</b> , <b>UDR</b> , <b>NSSF</b> , <b>SMSF</b> , <b>EIR</b> , <b>CHF</b> , <b>SEPP</b> , <b>AMF</b> , <b>UDM</b> , <b>NEF</b> , <b>SMF</b> , <b>SCP</b> .
IP Address	Set the IP address of the peer node.
IP Prefix	The IP address prefix assigned to this range. It specifies the number of leftmost bits

<b>Setting</b>	<b>Description</b>
Length	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:

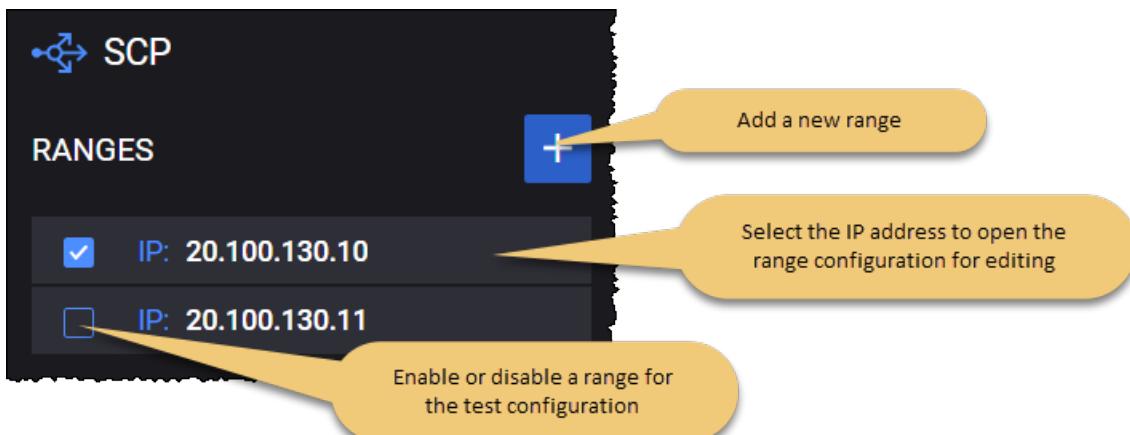
<b>SCP Ranges panel</b>	<b>463</b>
<b>SCP Range panel</b>	<b>464</b>
<b>SCP Node Settings</b>	<b>465</b>
<b>SCP Nscp interface settings</b>	<b>465</b>
<b>SCP Remote SBA Nodes</b>	<b>468</b>

## 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 ...



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All Ranges on All Agents**

## 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 <b>Delete Range</b> 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 (when range is not set as DUT):</i>	
Node Settings	Each SCP range requires the configuration of an associated set of Node Settings, which are described in <a href="#">SCP Node Settings</a> .
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 <a href="#">SCP interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">SCP Remote SBA Nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nscp IP Address	The IP address from your test network to use for traffic on this interface.
TLS Server Name	The name of the server to be sent in SNI extension header in TLS Client Hello message.

## SCP 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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
PLMN MCC	<p>The PLMN MCC for this PCF range.</p> <p><b>About PLMN MCC ...</b></p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this PCF range.</p> <p><b>About PLMN MNC ...</b></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>
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.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## SCP Nscp interface settings

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

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

The following **Security Settings** enable the necessary Nscp security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
<i>mTLS Client Settings</i>	Select the check-box to make this option available, and then select the <i>mTLS Client Settings</i> to open the configuration panel for editing.
<i>Certificates and Private Keys (.zip)</i>	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Role Name</i>	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>mTLS Server Settings</i>	<p><b>IMPORTANT</b> This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</p> <p>Select the check-box to make this option available, and then select the <i>mTLS Server Settings</i> to open the configuration panel for editing.</p>
<i>CA Certificate</i>	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Certificates and Private Keys (.zip)</i>	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Role Name</i>	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>Use Secrets Management System</i>	If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.

Security Settings	Description
	<p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other then the one selected in Active Root Certificate.
	<p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## SCP Remote SBA Nodes

### Peer SCP Type

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

### SCP Connection Settings

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

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

## NRF Connection Settings

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

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

## DNS Server Connection Settings

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.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

## 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:**

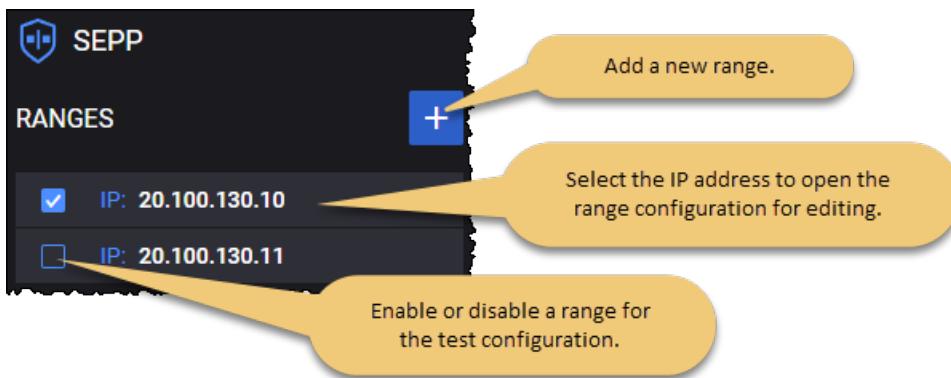
<b>SEPP Ranges panel</b> .....	<b>470</b>
<b>SEPP Range panel</b> .....	<b>471</b>
<b>SEPP Node Settings</b> .....	<b>472</b>
<b>SEPP Custom NF Services settings</b> .....	<b>473</b>
<b>SEPP Nsepp interface settings</b> .....	<b>473</b>
<b>SEPP Remote SBA Nodes</b> .....	<b>476</b>

### 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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on One Agent**

**IMPORTANT** The number of enabled SEPP ranges must be equal to the number of assigned agents.

## 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 <b>Delete Range</b> 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 <a href="#">SEPP Node Settings</a> .

Setting	Description
Custom NF Services	<p><b>IMPORTANT</b> This option appears if the range is set as DUT.</p> <p>This option will allow the configuration of a list of service parameters. See <a href="#">SEPP Custom NF Services settings</a> for more information.</p>
Nsepp Interface Settings	Each SEPP range requires the configuration of an interface necessary for SEPP connectivity. These settings are described in <a href="#">SEPP interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">SEPP Remote SBA Nodes</a> .
TLS Server Name	<p><b>IMPORTANT</b> This option appears only if the range is set as DUT.</p> <p>The name of the server to be sent in SNI extension header in TLS Client Hello message.</p>

## 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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
Name	The name of the SEPP range. You can accept the name provided by the LoadCore, or you can replace it with a name of your own choosing.
PLMN MCC	<p>The PLMN MCC for this range.</p> <p><b>About PLMN MCC ...</b></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 range.</p> <p><b>About PLMN MNC ...</b></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</p>

Setting	Description
	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.
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.
HTTP2 User Agent	User Agent header in HTTP2 requests initiated from this node. See 3GPP TS 29500, Table 5.2.2.2-1 for more information.

## SEPP Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the apiRoot for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## SEPP Nsepp interface settings

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

<b>Connectivity Settings</b>	<b>Description</b>
<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.
Gateway Address	The IP address assigned as 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.

The following **Security Settings** enable the necessary Nsepp security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
<i>mTLS Client</i>	<i>Select the check-box to make this option available, and then select the mTLS</i>

<b>Security Settings</b>	<b>Description</b>
<i>Settings</i>	<i>Client Settings to open the configuration panel for editing.</i>
Certificates and Private Keys (.zip )	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
CA Certificate	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>

Security Settings	Description
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate. <b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.

## 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>	
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 <b>Add Peer SEPP</b> button to add a new peer SEPP to your test configuration.
<i>Peer SEPP:</i>	
	Select the <b>Delete Peer SEPP</b> button to delete the peerSEPP range from your test configuration.
Peer SEPP	Select the IP address of the peer SEPP.

<b>Setting</b>	<b>Description</b>
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**.

<b>Setting</b>	<b>Description</b>
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.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

## 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:

<b>SGW Ranges panel</b> .....	<b>479</b>
<b>SGW Range panel</b> .....	<b>480</b>
<b>SGW S1-U Interface Settings</b> .....	<b>481</b>
<b>SGW S5-C Interface Settings</b> .....	<b>482</b>
<b>SGW S5-U Interface Settings</b> .....	<b>483</b>
<b>SGW S11 Interface Settings</b> .....	<b>484</b>
<b>SGW DUT S11 Interface Settings</b> .....	<b>485</b>

## SGW Ranges panel

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

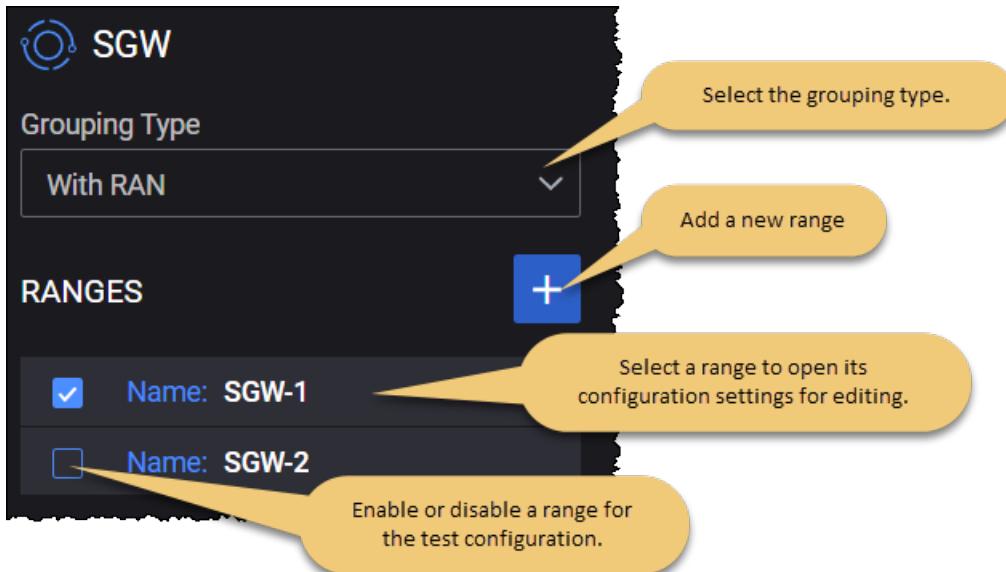
The following configuration option is available on this panel:

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

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 <b>Delete Range</b> 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><b>IMPORTANT</b> This field is available only when the <a href="#">Grouping Type</a> is set to <b>Standalone</b> and the SGW range is simulated.</p> <p>Size of receive buffers for UDP sockets:</p> <ul style="list-style-type: none"> <li>• minimum: 212992 #The default Linux buffer size</li> <li>• maximum: 134217728 #128MB</li> <li>• default: 12582912 #12MB</li> </ul>
UDP Tx Buffer (bytes)	<p><b>IMPORTANT</b> This field is available only when the <a href="#">Grouping Type</a> is set to <b>Standalone</b> and the SGW range is simulated.</p> <p>Size of transmit buffers for UDP sockets:</p> <ul style="list-style-type: none"> <li>• minimum: 212992 # The default Linux buffer size</li> <li>• maximum: 134217728 #128MB</li> <li>• default: 2097152 #2MB</li> </ul>
S1-u Interface Settings	These settings are described in <a href="#">SGW S1-U interface settings</a> .
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 <a href="#">SGW S5-C interface settings</a> .
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 <a href="#">SGW S5-U interface settings</a> .
S11 Interface Settings	These settings are described in <a href="#">SGW S11 interface settings</a> .
DUT S11 Interface Settings	These settings are described in <a href="#">SGW DUT S11 interface settings</a> .

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.

<b>Connectivity setting</b>	<b>Description</b>
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

### Interface Settings

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

<b>Interface setting</b>	<b>Description</b>
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.
GTP-C Destination UDP Port	Specify the UDP port that will be used for GTP-C message transmission. Value should be in range of 1024 to 65535.

### Connectivity Settings

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

<b>Connectivity setting</b>	<b>Description</b>
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	The IP address assigned as gateway address.

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

## 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.

<b>Connectivity setting</b>	<b>Description</b>
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).

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

## 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.

<b>Interface setting</b>	<b>Description</b>
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.
GTP-C Destination UDP Port	Specify the UDP port that will be used for GTP-C message transmission. Value should be in range of 1024 to 65535.

## Connectivity Settings

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

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

## 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:

<b>SMF/PGW-C Ranges panel</b>	<b>487</b>
<b>SMF/PGW-C Range settings</b>	<b>488</b>
<b>SMF Node settings</b>	<b>489</b>
<b>SMF Custom NF Services settings</b>	<b>491</b>
<b>SMF N4/Sx interface settings</b>	<b>491</b>
<b>SMF Nsmf interface settings</b>	<b>493</b>
<b>SMF Gx Interface settings</b>	<b>496</b>
<b>SMF S5-c interface settings</b>	<b>499</b>
<b>SMF remote SBA nodes</b>	<b>500</b>
<b>SMF Uplink Paths settings</b>	<b>505</b>
<b>SMF Slice and UPF Mapping settings</b>	<b>506</b>
<b>SMF EAS Deploy Subscription settings</b>	<b>506</b>
<b>SMF EAS Procedures Settings</b>	<b>507</b>

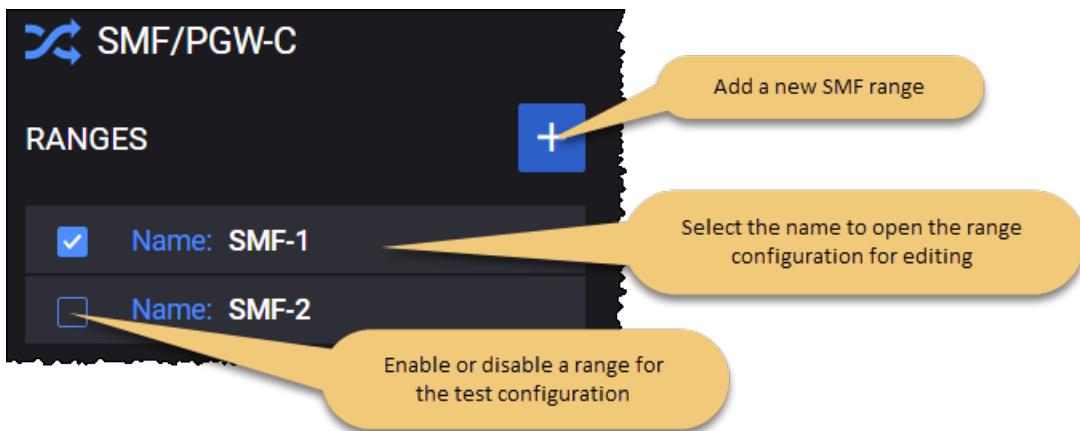
## SMF/PGW-C Ranges panel

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 ...**



If multiple agents are assigned to the SMF node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT** Only one SMF range can be configured on one agent.

- in case of multiple agents assigned and one Range defined, the range will be configured on each agent.
- in case of multiple agents and multiple ranges, each range can be configured on one agent.

## 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 <b>Delete Range</b> 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>	
RAT Type	This option allows you to enable only the functionalities specific to the selected Radio Access Technology type (RAT). Options available are: <b>5G</b> , <b>4G</b> , or <b>5G and 4G</b> . <div style="margin-top: 10px;"> <b>NOTE</b> Only the 4G option supports Gx Interface for 4G Stand Alone Core Network. The other options use the Dual Core Network which uses SBA interface between SMF/ (S)PGW-C and PCF.           </div>
Node Settings	Each SMF range requires the configuration of an associated set of Node Settings, which are described in <a href="#">SMF node settings</a> .
Custom NF Services	<div style="display: flex; align-items: center;"> <span style="background-color: #0070C0; color: white; padding: 2px 10px; font-weight: bold;">IMPORTANT</span> <span style="margin-left: 10px;">This option appears if the range is set as DUT.</span> </div> This option will allow the configuration of a list of service parameters. See <a href="#">SMF Custom NF Services settings</a> for more information.
N4/Sx 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 <a href="#">SMF N4 interface settings</a> .
Nsmf Interface Settings	Each SMF range requires the configuration of Nsmf interface settings, through which a SMF instance enables connectivity and interaction with

<b>Setting</b>	<b>Description</b>
	other functions in the 5G network. These settings are described in <a href="#">SMF Nsmf interface settings</a> .
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 <a href="#">SMF S5-c interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">SMF remote SBA nodes</a> .
Uplink Paths	These settings are described in <a href="#">SMF Uplink Paths settings</a> .
Slice and UPF Mapping	These settings are described in <a href="#">SMF Slice and UPF Mapping settings on page 506</a> .
EAS Deploy Subscription	<p>These settings are described in <a href="#">SMF EAS Deploy Subscription settings</a></p> <p><b>IMPORTANT</b> This option is available only if the <b>Technical Version Spec</b> from Global Settings is set to <b>R17 December 2022</b>.</p>
EAS Procedures Settings	<p>These settings are described in <a href="#">SMF EAS Procedures Settings</a>.</p> <p><b>IMPORTANT</b> This option is available only if the <b>Technical Version Spec</b> from Global Settings is set to <b>R17 December 2022</b>.</p>
TLS Server Name	<p><b>IMPORTANT</b> This option appears only if the range is set as DUT.</p> <p>The name of the server to be sent in SNI extension header in TLS Client Hello message.</p>

## 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.

<b>Setting</b>	<b>Description</b>
<i>Node Settings:</i>	
Instance ID	<p>Multiple SMF instances may be deployed in the 5G network.</p> <p>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.</p>
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.

Setting	Description
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 AMF Events	Select the check box in order to enable this option.
Request Shared Data	If enabled, the SMF will send a GET request to UDM for /nudm-sdm/v2/shared-data?shared-data-ids=12345-id (where 12345-id will be replaced with the value of shared data ID received in response to GET /nudm-sdm/v2/[SUPI]/sm-data).
UDP Rx Buffer (bytes)	The size in bytes of the receive buffers for UDP sockets: <ul style="list-style-type: none"> <li>minimum: 212992</li> <li>maximum: 134217728</li> <li>default: 12582912</li> </ul>
UDP Tx Buffer (bytes)	The size in bytes of the transmit buffers for UDP sockets: <ul style="list-style-type: none"> <li>minimum: 212992</li> <li>maximum: 134217728</li> <li>default: 2097152</li> </ul>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
Cache NRF Response	<p><b>IMPORTANT</b> This option appears only if the NRF node is enabled and the <a href="#">Peer NRF</a> value under <a href="#">Remote SBA Nodes &gt; NRF Connections Settings</a> is set.</p> <p>Select from the drop-down for how long to save/remember the peer SBA nodes that are discovered via NRF:</p> <ul style="list-style-type: none"> <li><b>Cache Permanently</b> (default)</li> <li><b>Don't Cache Responses</b></li> </ul>
3GPP RADIUS Client	Select to enable and set the RADIUS Client configuration for SMF.

Setting	Description
	<p><b>NOTE</b> <i>For information on the configuration of 3GPP RADIUS Server, see <a href="#">3GPP RADIUS Server configuration on page 135</a>.</i></p>
IP Address	The local IP Address used by the RADIUS Client simulated on the SMF node.
IP Address Count	The number of local IP addresses used by the RADIUS Client simulated on the SMF node. The increment for the IP addresses is 1.
Authentication Port	The local port used by the RADIUS Client simulated on the SMF node for the RADIUS 3GPP Authentication messages sent towards the RADIUS Server.
Accounting Port	The local port used by the RADIUS Client simulated on the SMF node for the RADIUS 3GPP Accounting messages sent towards the RADIUS Server.

## SMF Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## SMF N4/Sx 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/Sx Interface Settings:</i>	
Peer UPF	Select the UPF node or UPF nodes connected to SMF over the N4 interface. Available options include: <ul style="list-style-type: none"> <li>• <b>Discover</b> - visible only if the <b>RAT Type</b> is set to <b>5G</b> or <b>5G and 4G</b>. It will invoke the <a href="#">NF Discovery service</a>. Also, the NRF node must be selected in Remote SBA Nodes.</li> <li>• Select the IP address of the UPF node - This is the destination address of the UPF node to which the packets are sent over the Nupf interface.</li> <li>• <b>Select All</b> - used in case this SMF range connects to all defined UPF ranges.</li> </ul>
Include 3GPP Interface Type	Select this check box to include the 3GPP interface type in PFCP messages.
Enable SLAAC	Select to enable and configure the Stateless Address Auto-configuration (SLAAC) support on SMF/PGWc. The SMF/PGWc will include PDRs and FAR for handling of RS/RA messages in PFCP Session for either IPv6 or IPv4v6 PDU Session.
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.

**NOTE**

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

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

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

## 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.

<b>Connectivity Settings</b>	<b>Description</b>
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 <i>Gateway Address</i> ).

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

The following **Security Settings** enable the necessary Nsmf security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
mTLS Client Settings	<i>Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.</i>
Certificates and Private Keys (.zip )	You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.

<b>Security Settings</b>	<b>Description</b>
	<p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
CA Certificate	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	<p>Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.</p>
Active Root	<p>Select from the list one of the CA Certificate-type secret management system</p>

Security Settings	Description
Certificate	from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other than the one selected in Active Root Certificate. <b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.

## SMF Gx Interface settings

**IMPORTANT** This menu is available only if **RAT Type** value under [SMF/PGW-C Range settings](#) is set to **4G**.

Setting	Description
<i>Gx Interface Settings</i>	
Peer PCRF	Select the IP address of the PCRF node.
Diameter Settings	<i>Select to open the Diameter settings panel.</i>
Origin Host Prefix	Set the origin host prefix. Default value: <b>host</b> .
Origin Realm	Set the origin realm. Default value: <b>keysight.com</b> .
Destination Host	Set the destination host prefix.
Destination Realm	Set the destination realm.
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.
Destination SCTP Port	The destination Stream Control Transmission Protocol (SCTP) port for control plane messages (NG-AP signaling messages) on the Gx interface.
Diameter Transport	Select the diameter transport type: <b>SCTP</b> or <b>TCP</b> .
SCTP Parameters	<i>Select to open the configuration panel.</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.

<b>Setting</b>	<b>Description</b>
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.
<i>SCTP Buffers</i>	<i>Select to open the configuration panel.</i>
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the SCTP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for SCTP sockets.
<i>TCP Parameters</i>	<i>Select to open the configuration panel.</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.
Maximum Segment Size (MSS)	<p>The desired Maximum Segment Size (MSS) for the 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>
Use timestamps	Turn on to enable timestamps on TCP packets.

<b>Setting</b>	<b>Description</b>
TCP Buffers	<i>Select to open the configuration panel.</i>
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the TCP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for TCP sockets.
<i>Connectivity Settings</i>	
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).
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.
Gateway Address	The IP address assigned as 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.

Setting	Description
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

## 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

### 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.
GTP-C Destination UDP Port	Specify the UDP port that will be used for GTP-C message transmission. Value should be in range of 1024 to 65535.

### Connectivity 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
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.

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

## SMF remote SBA nodes

### AMF Connection Settings

<b>Setting</b>	<b>Description</b>
<i>AMF Connectivity Settings:</i>	
Peer AMF Type	<p>Select one of the available options:</p> <ul style="list-style-type: none"> <li>• <b>Preset</b></li> <li>• <b>Discover</b></li> </ul> <p>More details <a href="#">below</a>.</p>
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer AMF Type is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a>.</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	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"> <li>• 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.</li> <li>• Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> Refer to <a href="#">NF Discovery service</a> 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	<p>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.</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"> <li>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.</li> <li>Select <b>Discover</b> to invoke the NF discovery service. Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</li> </ul>
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.

## EASDF Connection Settings

**IMPORTANT** This option becomes available only if the **Technical Spec Version** from Global Settings is set to **R17 December 2022**.

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

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

## NRF Connection Settings

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

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

## DNS Server Connection Settings

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.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

## NEF Connection Settings

**IMPORTANT** This option becomes available for configuration only if the **Technical Spec Version** from Global Settings is set to **R17 December 2022**.

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

Setting	Description
<i>NEF Connection Settings:</i>	
Peer NEF	Select either the IP address of an NEF from your test network or <i>None</i> if you are not using an NEF in your test configuration. The IP address is the destination address of the NEF node to which the packets are sent over the Nnrf interface.
Protocol	The protocol to use for Nnef communications. It can be either <b>HTTP</b> or <b>HTTPS</b> .
Port	The port number to use for Nnef 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"> <li>• <b>Telescopic FQDN</b></li> <li>• <b>Target API Root</b></li> </ul>

## Home PLMN for Inter-PLMN Routing

The following configuration settings are required.

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

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

Setting	Description
<i>Uplink Paths:</i>	
	Select the <b>Add an uplink path</b> button to add an uplink path to your test configuration.
<i>Uplink Path:</i>	
	Select the <b>Delete uplink path</b> button to remove the uplink path from your test configuration.
N3 UPF	Select the first UPF in Uplink User Plane path, the UPF connected to RAN.
Use Uplink Classifier UPF	<p><b>IMPORTANT</b> <i>This option appears when an UPF is selected in the N3 UPF drop-down and the Technical Spec Version is set to R17 December 2022.</i></p> <p><i>If enabled, it will allow you to configure how to use the Uplink Classifier UPF.</i></p>
Local PSA-UPF	Select from the list the UPF used for traffic towards Edge Application Server.
QoS Flow(s) for	Select from the list the QoS Flows used for traffic towards Edge Application

Setting	Description
Local PSA-UPF	Server (multiple choices are allowed).
Central PSA-UPF	Select from the list the UPF used for Initial PDU Session Establishment and that, after ULCL insertion, will be used to forward all non-Edge Application traffic.
QoS Flow(s) for Central PSA-UPF	Select from the list the QoS Flows used for non-Edge Application traffic.

## SMF Slice and UPF Mapping settings

The following table describes the Slice and UPF Mapping settings.

Setting	Description
<i>SMF Slice and UPF Mapping:</i>	
	Select the <b>Add Slice and UPF Mapping</b> button to add a network slice to your test configuration.
<i>SMF NSSAI:</i>	
	Select the <b>Delete Slice and UPF Mapping</b> button to remove this network slice from your test configuration.
SST	The Slice/Service Type (SST) value for this network slice.
SD	The Slice/Service Type (SST) value for this network slice. 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	One or more DNNs (Data Network Names) associated with the network slice and uplink path. Select one or more DNNs from the drop-down list.
Uplink Path	Select the uplink path from the drop-down list. Note that only the <a href="#">Uplink Path</a> entries without <b>Use Uplink Classifier UPF</b> enabled will appear in the list.

## SMF EAS Deploy Subscription settings

**IMPORTANT** This option is available only if the **Technical Version Spec** from Global Settings is set to **R17 December 2022**.

The following table describes the settings required to configure the EAS Deploy Subscription.

Setting	Description
<i>EAS Deploy Subscription:</i>	

Setting	Description
	Select the <b>Add an EAS Deploy Subscription</b> button to add a subscription configuration to your test configuration.
<i>EAS Deploy Subscriptions:</i>	
	Select the <b>Delete EAS Deploy Subscription</b> button to remove the current subscription from your test configuration.
DNN SNSSAI Information	<i>Add and configure the DNN SNSSAI used with EAS deploy subscription. See configuration details in the <a href="#">DNN SNSSAI Information configuration below</a> table.</i>
Application ID	Identifies the application to which the EAS Deployment Information corresponds.
Immediate Report	If enabled, it requires the immediate reporting of the current status of EAS Deployment Information, if available. When disabled (default), the EAS Deployment Information event report occurs when the event is met.
Internal Group ID	This parameter is used to identify an internal group.

### DNN SNSSAI Information configuration

Setting	Description
<i>DNN SNSSAI Information:</i>	
	Select the <b>Add an DNN SNSSAI Information</b> button to add the SNSSAI information to your test configuration.
<i>DNN SNSSAI Information:</i>	
	Select the <b>Delete DNN SNSSAI Information</b> button to remove the SNSSAI information 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.
DNN	The DNN (Data Network Name) with which PDU sessions will be associated for this SNSSAI.

### SMF EAS Procedures Settings

**IMPORTANT** This option is available only if the **Technical Version Spec** from Global Settings is set to **R17 December 2022**.

The following table describes the settings required to configure the EAS Procedures Settings.

Setting	Description
<i>EAS Procedure Settings:</i>	
 +	Select the <b>Add EAS Procedures Settings</b> button to add a new EAS (Re)Discovery Procedure entry in the test configuration.
<i>EAS Procedure Settings:</i>	
	Select the <b>Delete EAS Procedures Settings</b> button to delete an EAS (Re)Discovery Procedure entry from the test configuration.
Procedures	Select from the drop-down the type of procedure to configure: <ul style="list-style-type: none"> <li>• EAS Discovery</li> <li>• EAS Rediscovery</li> </ul>
EAS IP Address	Add the Edge Application Server IP Address. <p><b>IMPORTANT</b> This parameter appears only if Procedures is set to EAS Discovery.</p>
Uplink Path	Select from the drop-down the uplink path associated with the EAS IP. Note that only the <u>Uplink Path</u> entries <u>with Use Uplink Classifier UPF</u> enabled will appear in the list.
Procedure Trigger	Select from the drop-down what action will trigger the current procedure: <ul style="list-style-type: none"> <li>• TAC Change</li> <li>• DNAI Change</li> </ul> <p><b>IMPORTANT</b> This parameter appears only if Procedures is set to EAS Rediscovery.</p>
DNS Server	The IPv4/IPv6 DNS server address associated with the TAC List/DNAI server. <p><b>IMPORTANT</b> This parameter appears only if Procedures is set to EAS Rediscovery.</p>
TACS	Define one or more TAC Lists values that employ the same Uplink Path and DNS Server. It is expected to have at least one TAC value (list of integers 0 – 16777215). Use  + to add multiple TAC values. <p><b>IMPORTANT</b> This parameter appears only if Procedures is set to EAS Rediscovery, and Procedure Trigger is set to <i>TAC Change</i>.</p>
DNAI	The DNAI value that employs the Uplink Path and DNS Server. <p><b>IMPORTANT</b> This parameter appears only if Procedures is set to EAS Rediscovery, and Procedure Trigger is set to <i>DNAI Change</i>.</p>

# 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:

<b>SMSF Ranges panel</b>	<b>509</b>
<b>SMSF Range panel</b>	<b>510</b>
<b>SMSF Node settings</b>	<b>511</b>
<b>SMSF Nsmsf interface settings</b>	<b>511</b>
<b>SMSF Remote SBA Nodes</b>	<b>514</b>

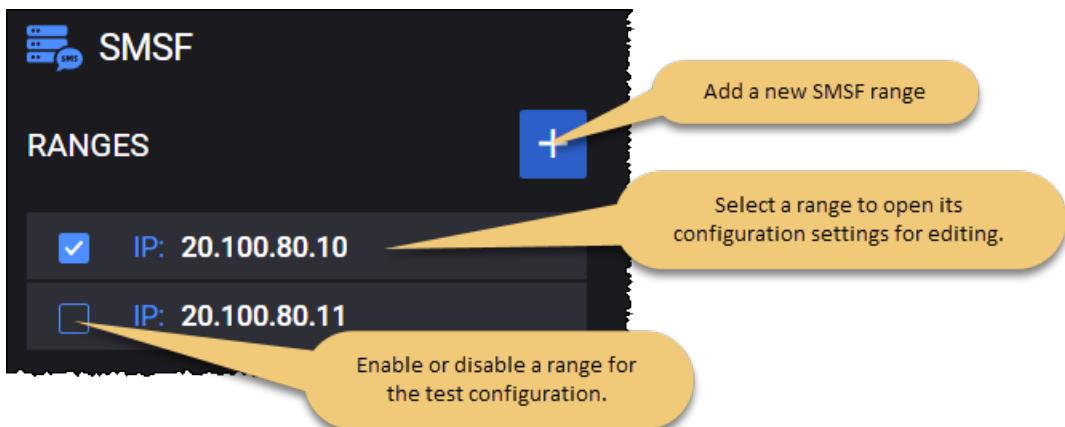
## SMSF Ranges panel

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 ...



If multiple agents are assigned to the SMSF node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT**

Only one SMSF range can be configured on one agent.

- in case of multiple ranges, it will require one agent for each range;
- in case one range and multiple agents, each agent will create a different SMSF NF, with incremented IP address and NF ID, and whole UE range.

## 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 <b>Delete Range</b> 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 <a href="#">SMSF node settings</a> .
Nsmsf 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 <a href="#">SMSF Nsmsf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">SMSF remote SBA nodes</a> .
DUT Nsmsf IP Address	<div style="background-color: #0070C0; color: white; padding: 2px 10px; display: inline-block;"> <b>IMPORTANT</b> </div> This parameter appears only if the range is set as DUT. The IP address from your test network to use for traffic on this interface.

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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
PLMN MCC	<p>The PLMN MCC for this AMF range.</p> <p><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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.

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

The following **Security Settings** enable the necessary Nsmsf security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
<i>mTLS Client Settings</i>	Select the check-box to make this option available, and then select the <i>mTLS Client Settings</i> to open the configuration panel for editing.
<i>Certificates and Private Keys (.zip)</i>	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Role Name</i>	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>mTLS Server Settings</i>	<p><b>IMPORTANT</b> This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</p> <p>Select the check-box to make this option available, and then select the <i>mTLS Server Settings</i> to open the configuration panel for editing.</p>
<i>CA Certificate</i>	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Certificates and Private Keys (.zip)</i>	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
<i>Role Name</i>	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>Use Secrets Management System</i>	If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.

Security Settings	Description
	<p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other then the one selected in Active Root Certificate.
	<p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## SMSF Remote SBA Nodes

### AMF Connection Settings

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

Setting	Description
<i>AMF Connectivity Settings:</i>	
Peer AMF type	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> <li>• Select <b>Preset</b> - this option allows manually configuration of a peer AMF, as described <a href="#">here</a>.</li> <li>• Select <b>Discover</b> to invoke the NF discovery service. The SMSF will discover the AMF.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer AMF is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a>.</p>

The following table describes the settings required to configure a preset peer AMF:

Setting	Description
<i>AMF Peers:</i>	
	Select this button to add the peer AMF to your test configuration.
<i>AMF Peer:</i>	
	Select this button to delete the peer AMF from your test configuration.
Peer AMF	Select the peer AMF from the drop-down list.
Protocol	The protocol to use for Namf communications. It can be either HTTP or HTTPS.
Port	The AMF port number to use for Namf communications. The default is port 80, but you can choose a different port number.
<b>NOTE</b> In Full Core topology, in order for SMSF to establish a connection with a DUT AMF, the Full Core AMF marked as DUT should be configured with an IP and Instance ID that match the ones of the real AMF.	

## UDM Connection Settings

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

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM type	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> <li>Select <b>None</b> - no N21 interface.</li> <li>Select <b>Preset</b> - active N21 interface, this option allows manually configuration of a peer UDM, as described <a href="#">here</a>.</li> <li>Select <b>Discover</b> - active N21 interface, the peer UDM is discovered via NRF.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer UDM is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p>

Setting	Description
	Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a> .

The following table describes the settings required to configure a preset peer UDM:

Setting	Description
<i>UDM Peers:</i>	
	Select this button to add the peer UDM to your test configuration.
<i>UDM Peer:</i>	
	Select this button to delete the peer UDM from your test configuration.
Peer UDM	Select the peer UDM 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.

## 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.

## DNS Server Connection Settings

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.

Setting	Description
Port	The port number to use for communications.
DNS Entry Cache Expiry (s)	The interval (in seconds) after which the cached DNS entries will be deleted; the DNS resolving of producer FQDN will be performed again. A zero value means this setting is disabled.

## 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.

# 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:

<b>UDM/HSS Ranges panel</b>	<b>519</b>
<b>UDM/HSS Range panel</b>	<b>520</b>
<b>UDM Range Settings</b>	<b>521</b>
UDM Settings	521
UDM Node Settings	522
UDM/HSS Custom NF Services settings	525
UDM Nudm Interface Settings	526
UDM Remote SBA Nodes	528
<b>HSS Range Settings</b>	<b>530</b>
HSS Settings	530
HSS Node Settings	531
HSS S6a Interface Settings	532
<b>UDM and HSS Range Settings</b>	<b>534</b>
<b>UDM/HSS Custom NF Services settings</b>	<b>535</b>

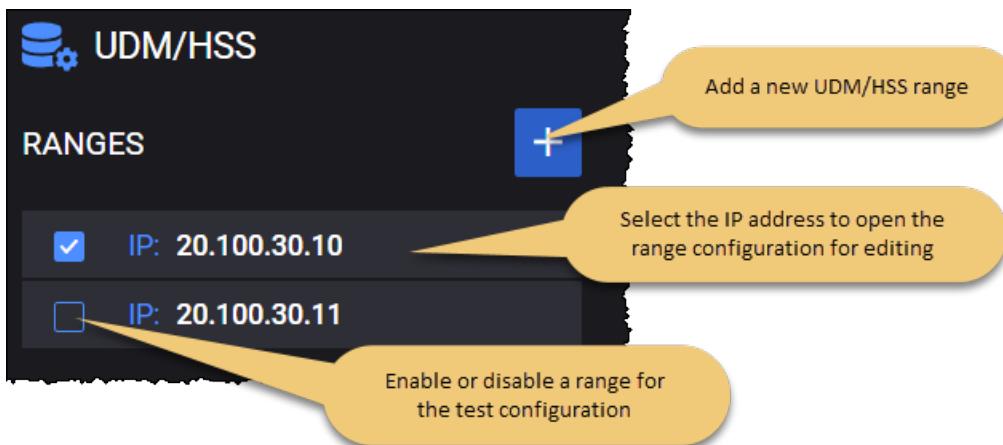
## UDM/HSS Ranges panel

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 ...**



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT**

Only one UDM/HSS range can be configured on one agent.

- in case of multiple ranges, it will require one agent for each range;
- in case one range and multiple agents, each agent will create a different UDM NF, with incremented IP address and NF ID, and whole UE range.

## 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 <b>Delete Range</b> 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 ( <b>UDM</b> , <b>HSS</b> or <b>UDM and HSS</b> ) 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"> <li>• <a href="#">UDM Range Settings</a></li> <li>• <a href="#">HSS Range Settings</a></li> <li>• <a href="#">UDM and HSS Settings</a></li> </ul>
<i>Range Settings (when range is set as DUT):</i>	
DUT S6a IP Address	The IP address from your test network to use for traffic on this interface.
Custom NF Services	This option will allow the configuration of a list of service parameters. See <a href="#">UDM/HSS Custom NF Services settings</a> for more information.

## UDM Range Settings

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

Setting	Description
<i>Range Settings (when range is not set as DUT):</i>	
Settings	Each UDM range requires the configuration of an associated set of Settings, which are described in <a href="#">UDM settings</a> .
UDM Node Settings	Each UDM range requires the configuration of an associated set of Node Settings, which are described in <a href="#">UDM node settings</a> .
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 <a href="#">UDM Nudm interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">Remote SBA nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nudm IP Address	The IP address from your test network to use for traffic on this interface.
Custom NF Services	This option will allow the configuration of a list of service parameters. See <a href="#">UDM/HSS Custom NF Services settings</a> for more information.
TLS Server Name	The name of the server to be sent in SNI extension header in TLS Client Hello message.

## 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><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></p>

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.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
<i>Network Initiated Deregistration: You can enable or disable this option, as required by your test configuration.</i>	
Delay	Set the delay value.
Trigger	Describes what triggers the sending of the Network Deregistration message. Available options: <ul style="list-style-type: none"><li>• <b>Subscribe</b> - AMF to UDM SDM subscription HTTP procedure</li><li>• <b>Update Location</b> - MME to HSS Update Location Request Diameter procedure</li></ul>
Deregistration Reason	Select the deregistration reason from the drop-down list. Available options: <ul style="list-style-type: none"><li>• UE INITIAL REGISTRATION</li><li>• UE REGISTRATION AREA CHANGE</li><li>• SUBSCRIPTION WITHDRAWN</li><li>• 5GS TO EPS MOBILITY</li><li>• 5GS TO EPS MOBILITY UE INITIAL REGISTRATION</li><li>• REREGISTRATION REQUIRED</li></ul>

## 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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
Home Network	The Home Network Private key that is used for subscriber privacy. The Subscription identifier de-concealing function (SIDF)—which is a service

Setting	Description
Private key	<p>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><b>About SUPI and SUCI ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
<i>Routing Indicators: For details, refer to <a href="#">Routing Indicators</a>.</i>	
<i>SDM Notifications: For details, refer to <a href="#">SDM Notifications</a>.</i>	

## 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 <b>Add Routing Indicator</b> button to add a Routing Indicator for the UDM range.
	Select the <b>Delete</b> 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 <b>Delete Subscription</b> button to remove this subscription from the SDM notifications.
Resource name	This represents the subscribed resource (entered as a string) for which notifications are triggered. Valid strings currently supported: <i>nssai, am-data, smf-select-data, sm-data, ue-context-in-smf-data</i> .
Notification trigger time (ms)	This represents the time interval (in milliseconds) from NF subscription (for that resource) after which that NF will start receiving notifications from UDM.
Change resource continuously	Select this option to apply the changes from the list continuously(start over again when reaching the end of the list). If this option is not selected, the notifications for the resource will stop when the last change in the list will happen, otherwise they will start from the beginning again.
<i>Resource changes:</i>	
	Select the <b>Add change</b> button to add new list of changes that will happen over time to the defined resource.
<i>Change Item</i>	
	Select the <b>Delete Change Item</b> to remove this list from your configuration.
Change type	This represents the nature of the change: <ul style="list-style-type: none"> <li>• <b>Add</b> - new content was added to the resource.</li> <li>• <b>Replace</b> - a certain content was replaced.</li> <li>• <b>Remove</b> - a certain content was removed.</li> <li>• <b>Move</b> - a certain content has been moved from one place to another.</li> </ul>
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).

Setting	Description
New JSON value	<p>This represents the new JSON text value for the object identifier by the <a href="#">Path in resource to change</a>.</p> <p><b>IMPORTANT</b> This field must have a valid JSON text value only if the <a href="#">Change type</a> is set to <b>Add or Replace</b>.</p>
Trigger after previous notification change (ms)	<p>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 <a href="#">Notification Trigger timer</a>.</p>
From source path (used for Move change type)	<p><b>NOTE</b> This parameter is available only when <a href="#">Change type</a> is set to <b>Move</b>.</p> <p>This represents the original path of the JSON object that has been moved.</p>

## UDM/HSS Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## 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>	<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.
Gateway Address	The IP address assigned as 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.

Connectivity Settings	Description
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

The following **Security Settings** enable the necessary Nudm security interaction.

Security Settings	Description
<i>TLS Settings</i>	
mTLS Client Settings	Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
mTLS Server Settings	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</p>
CA Certificate	Select from the drop-down list one of the available server certificates.
	<p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRTand the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>

Security Settings	Description
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function Certificate	Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	<p>Select from the list one of the CA Certificate-type secret management system from global settings, other then the one selected in Active Root Certificate.</p> <p><b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.</p>

## 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 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.
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"> <li>• <b>Telescopic FQDN</b></li> <li>• <b>Target API Root</b></li> </ul>

## Home PLMN for Inter-PLMN Routing

The following configuration settings are required.

PLMN MCC	Provide the PLMN MCC value. <b>About PLMN MCC ...</b> 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
----------	--

	<p>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><b>About PLMN MNC ...</b></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 <a href="#">HSS settings</a> .
HSS Node Settings	Each HSS range requires the configuration of an associated set of Node Settings, which are described in <a href="#">HSS node settings</a> .
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 <a href="#">HSS S6a interface settings</a> .

## 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><b>About PLMN MCC ...</b></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	The PLMN MNC for this HSS range.

Setting	Description
	<p><b>About PLMN MNC ...</b></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"> <li>• <b>Subscribe</b> - AMF to UDM SDM subscription HTTP procedure</li> <li>• <b>Update Location</b> - MME to HSS Update Location Request Diameter procedure</li> </ul>
Deregistration Reason	<p>Select the deregistration reason from the drop-down list. Available options:</p> <ul style="list-style-type: none"> <li>• UE INITIAL REGISTRATION</li> <li>• UE REGISTRATION AREA CHANGE</li> <li>• SUBSCRIPTION WITHDRAWN</li> <li>• 5GS TO EPS MOBILITY</li> <li>• 5GS TO EPS MOBILITY UE INITIAL REGISTRATION</li> <li>• REREGISTRATION REQUIRED</li> </ul>

## HSS Node Settings

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

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

### Diameter Transport settings

Setting	Description
Diameter Transport	Select the diameter transport type: <b>SCTP</b> or <b>TCP</b> .
<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.
<i>SCTP Buffers</i>	
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the SCTP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for SCTP sockets.

<b>Setting</b>	<b>Description</b>
<i>TCP 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.
Maximum Segment Size (MSS)	The desired Maximum Segment Size (MSS) for the 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).
Use timestamps	Turn on to enable timestamps on TCP packets.
<i>TCP Buffers</i>	
Tx Buffers (bytes)	The size (in bytes) of transmit buffers for the TCP sockets.
Rx Buffers (bytes)	The size (in bytes) of receive buffers for TCP sockets.

The following **Connectivity Settings** enable the necessary S6a connectivity and service interaction.

<b>Connectivity Settings</b>	<b>Description</b>
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.
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>

<b>Connectivity Settings</b>	<b>Description</b>
	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.
Gateway Address	The IP address assigned as 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	<i>VLAN tag protocol ID.</i>
Inner VLAN	<p><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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.

<b>Setting</b>	<b>Description</b>
Settings	Each UDM and HSS range requires the configuration of an associated set of Settings, which are described in <a href="#">UDM settings</a> or <a href="#">HSS settings</a> .
UDM Node Settings	Each UDM and HSS range requires the configuration of an associated set of UDM Node Settings, which are described in <a href="#">UDM node settings</a> .

Setting	Description
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 <a href="#">UDM Nudm interface Settings</a> .
HSS Node Settings	Each UDM and HSS range requires the configuration of an associated set of HSS Node Settings, which are described in <a href="#">HSS node settings</a> .
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 <a href="#">HSS S6a interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">remote SBA nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nudm IP Address	The IP address from your test network to use for traffic on this interface.
DUT S6a IP Address	The IP address from your test network to use for traffic on this interface.
Custom NF Services	This option will allow the configuration of a list of service parameters. See <a href="#">UDM/HSS Custom NF Services settings</a> for more information.
TLS Server Name	The name of the server to be sent in SNI extension header in TLS Client Hello message.

## UDM/HSS Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

Setting	Description
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.

Setting	Description
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

# 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:

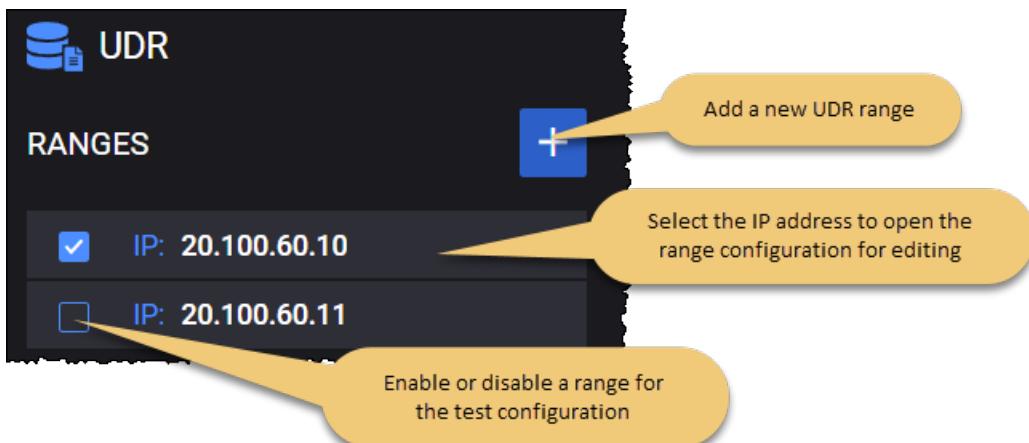
<b>UDR Ranges panel</b>	<b>537</b>
<b>UDR Range panel</b>	<b>538</b>
<b>UDR Node Settings</b>	<b>539</b>
<b>UDR Nudr interface settings</b>	<b>539</b>
<b>UDR Remote SBA Nodes</b>	<b>542</b>
<b>UDR Custom NF Services settings</b>	<b>542</b>

## 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 ...



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All Ranges on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT**

One or more UDR ranges can be configured on one agent.

- in case of one range and multiple agents, each agent will create a different UDR NF, with incremented IP address and NF ID, and a whole UE range;
- in case of round robin, each range will be configured on another agent.

## 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 <b>Delete Range</b> 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 (when range is not set as DUT):</i>	
Node Settings	Each UDR range requires the configuration of an associated set of Node Settings, which are described in <a href="#">UDR Node Settings</a> .
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 <a href="#">UDR Nudr interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">UDR remote SBA nodes</a> .
<i>Range Settings (when range is set as DUT):</i>	
DUT Nudr IP Address	The IP address from your test network to use for traffic on this interface.

Setting	Description
Custom NF Services	This option will allow the configuration of a list of service parameters. See <a href="#">UDR Custom NF Services settings</a> for more information.
TLS Server Name	The name of the server to be sent in SNI extension header in TLS Client Hello message.

## UDR 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.
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
Name	The name of the UDR range. You can accept the name provided by the LoadCore, or you can replace it with a name of your own choosing.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
PLMN MCC	Set the mobile country code.
PLMN MNC	Set the mobile network code.

## 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	The IP address assigned as gateway address.

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

The following **Security Settings** enable the necessary Nudr security interaction.

<b>Security Settings</b>	<b>Description</b>
<i>TLS Settings</i>	
<i>mTLS Client Settings</i>	<i>Select the check-box to make this option available, and then select the mTLS Client Settings to open the configuration panel for editing.</i>

<b>Security Settings</b>	<b>Description</b>
Certificates and Private Keys (.zip )	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRT and the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Client is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
<i>mTLS Server Settings</i>	<p><b>IMPORTANT</b> <i>This option is available only if the interface's <b>Protocol</b> parameter is set to <b>HTTPS</b>.</i></p> <p><i>Select the check-box to make this option available, and then select the mTLS Server Settings to open the configuration panel for editing.</i></p>
CA Certificate	<p>Select from the drop-down list one of the available server certificates.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Certificates and Private Keys (.zip)	<p>You can use the <b>Upload</b> button to add the archive that contains an equal number of CRT and KEY file types, where the CRTand the associated KEY file have the same name. Use <b>Clear</b> to remove the file, if necessary.</p> <p><b>IMPORTANT</b> This configuration of mTLS Server is available only if the <a href="#">Use Secrets Management System</a> is not enabled. See Role Name parameter if otherwise.</p>
Role Name	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Use Secrets Management System</a> is enabled.</p> <p>Add a role name, as mapped to the policy used to retrieve the root certificate from Vault. This field cannot be empty.</p>
Use Secrets Management System	<p>If enabled, it will allow configuration of the following parameters. This parameter appears only when mTLS Server and/or mTLS Client Settings options are selected for use.</p> <p><b>IMPORTANT</b> If this option is enabled, make sure you first configure the <a href="#">Secret Management System</a> under Global Settings. Otherwise, the following parameters will not include values for configuration, therefore enabling this setting becomes useless.</p>
Network Function	<p>Select from the list one of the Network Function TLS Certificate-type secret management system defined in Global Settings.</p>

<b>Security Settings</b>	<b>Description</b>
Certificate	
Active Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings. This parameter can be empty.
Staged Root Certificate	Select from the list one of the CA Certificate-type secret management system from global settings, other then the one selected in Active Root Certificate. <b>IMPORTANT</b> This parameter appears only if Active Root Certificate is not empty.

## UDR Remote SBA Nodes

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

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

## UDR Custom NF Services settings

**IMPORTANT** This option appears only if the range is set as DUT.

This option requires the configuration of the Custom NF Services, as follows:

<b>Setting</b>	<b>Description</b>
<i>Custom NF Services:</i>	
	Select this button to add a custom NF service to your test configuration.
<i>Custom NF Service:</i>	
	Select this button to delete the custom NF service from your test configuration.
Service Name	One of the service names defined in 3GPP TS 29510, Table: 6.1.6.3.11.

Setting	Description
Hostname	The hostname or IP address used to address the service in DUT Network Function. A custom hostname has to be configured in order to use custom Protocol and/or Port.
Protocol	The protocol used to address the service in DUT Network Function. It can be <b>HTTP</b> or <b>HTTPS</b> .
Port	The port used to address the service in DUT Network Function.
ApiPrefix	The ApiPrefix used to construct the <code>apiRoot</code> for the service in DUT Network Function. See 3GPP TS 29501 4.4.1 for details.

## 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:

<b>UPF/PGW-U Ranges panel</b>	<b>545</b>
<b>UPF/PGW-U Range panel</b>	<b>546</b>
<b>UPF Node settings</b>	<b>547</b>
<b>UPF N3 interface settings</b>	<b>547</b>
<b>UPF N4 interface settings</b>	<b>549</b>
<b>UPF N6 interface settings</b>	<b>550</b>
<b>UPF N9 interface settings</b>	<b>551</b>
<b>UPF Nupf Interface Settings</b>	<b>553</b>
<b>UPF N4u interface settings</b>	<b>554</b>
<b>UPF Remote SBA Nodes</b>	<b>556</b>
<b>UPF Slice Mapping settings</b>	<b>556</b>

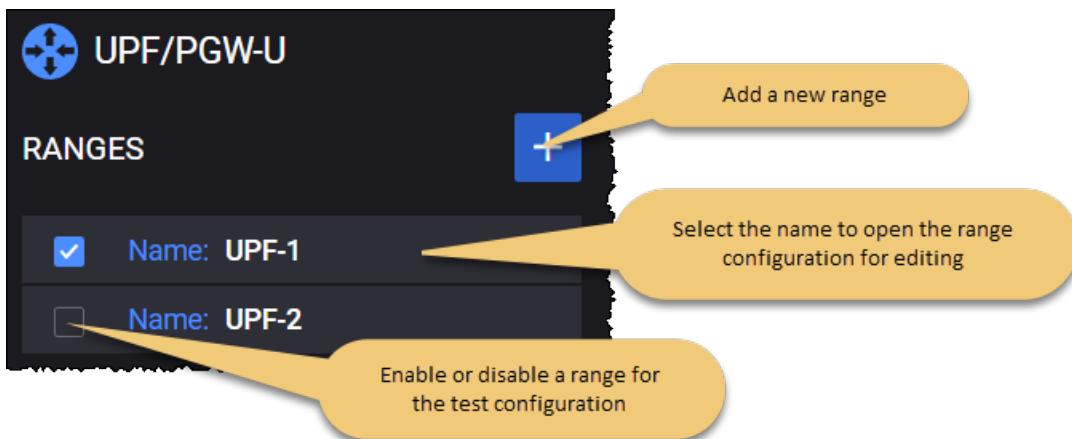
## UPF/PGW-U Ranges panel

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 Distribution Mode

UPF node allows you to chose whether to manually assign the agents, or use the standard (computed) Distribution Mode:

- If the **Manual Distribution** button is enabled, it will activate the UPF Ranges Column under the [Agent Assignment](#) window, where you can manually select to which range(s) an agent will be assigned.
- If this option is not enabled, it will go further with the **Computed Distribution Mode**, as explained in the following lines.

If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **All Ranges on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT** One or multiple UPF ranges can be configured on one agent.

If one or multiple ranges and multiple agents is the case, each range can be configured on one agent or each range can be configured on multiple agents incrementing IP address, etc.

## 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 <b>Delete Range</b> 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.
<i>Range Settings:</i>	
PSA-UPF	This option enables the UPF range as the PDU Session Anchor. The UPF will be connected to the DN. The toggle is switched on by default.
Node Settings	Each UPF range requires the configuration of an associated set of Node Settings, which are described in <a href="#">UPF Node settings</a> .
N3 Interface Settings	N3 is the interface between the RAN and the UPF. These interface settings are described in <a href="#">UPF N3 interface settings</a> .
N4 Interface Settings	N4 is the interface between the SMF and the UPF. These interface settings are described in <a href="#">UPF N4 interface settings</a> .
N6 Interface Settings	N6 is the interface between the DN and the UPF. These interface settings are described in <a href="#">UPF N6 interface settings</a> .
N9 Interface Settings	N9 is the interface between two UPFs. These interface settings are described in <a href="#">UPF N9 interface settings</a> .
Nupf	Each UPF range requires the configuration of Nupf interface settings, through which a

Setting	Description
Interface Settings	UPF instance enables connectivity and interaction with other functions in the 5G network. These settings are described in <a href="#">UPF Nupf interface settings</a> .
N4u Interface Settings	N4u is an interface between the SMF and the UPF. The interface settings are described in <a href="#">UPF N4u interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">UPF remote SBA nodes</a> .
Slice Mapping	These settings are described in <a href="#">UPF Slice Mapping settings</a> .

## UPF Node settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple UPF instances may be deployed in the 5G network. Each UPF 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 Mobile Country Code (MCC) for this UPF range.
PLMN MNC	The PLMN Mobile Network Code (MNC) for this UPF range.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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 <b>Add value</b> button to add a network instance to your test configuration.

Setting	Description
	Select the <b>Delete</b> 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>	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><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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>

<b>Connectivity Settings</b>	<b>Description</b>
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.

<b>Setting</b>	<b>Description</b>
<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.
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 <b>Supports FTEID Allocation</b> option is enabled.
Supports Send EndMarker	This option corresponds to the PFCP Association Setup Response > UP Function Features > EMPU flag.  If enabled, the UPF/PGW-U advertises its capability to send End Marker towards RAN. If disabled, the SMF/PWG-C may trigger the End Marker (if capable), and send it on the N4u interface so the UPF/PGW-U can redirect it towards RAN.

**NOTE**

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

<b>Connectivity Settings</b>	<b>Description</b>
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.

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

## 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.

<b>Connectivity Settings</b>	<b>Description</b>
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.

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><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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 <b>Add value</b> button to add a network instance to your test configuration.
	Select the <b>Delete</b> 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 <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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## UPF Nupf Interface Settings

Nupf 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 Nupf 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.
Gateway Address	The IP address assigned as 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.

Connectivity Settings	Description
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

## UPF N4u interface settings

The N4u interface is used to forward packets between SMF and UPF. It is used for SLAAC Procedure to forward RS and RA messages and for RADIUS procedures between RADIUS Client from SMF/PGWc and a RADIUS Server reachable via N6/SGi interface.

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 <b>Add value</b> button to add a network instance to your test configuration.
	Select the <b>Delete</b> 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.

<b>Connectivity Settings</b>	<b>Description</b>
<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.
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
<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.
Gateway Address	The IP address assigned as gateway address.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i> ). The default value is 000000000001.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
<i>Inner VLAN</i>	<b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.
VLAN TPID	VLAN tag protocol ID.

## UPF Remote SBA Nodes

**IMPORTANT** This section becomes available for configuration only if [Nupf interface settings](#) is selected in the range configuration list.

The following configuration settings are required.

Settings	Description
<i>NRF Connection Settings:</i>	
Peer NRF	Select the peer UPF using either of the following methods: <ul style="list-style-type: none"> <li>Select the IP address of the UPF node. This is the destination address of the UPF node to which the packets are sent over the Nupf interface.</li> <li><b>None</b></li> </ul>
Protocol	The protocol to use for Nudm communications. It can be either HTTP or HTTPS.
Port	The UPF port number to use for Nupf communications. The default is port 80, but you can choose a different port number.

## UPF Slice Mapping settings

**IMPORTANT** This section becomes available for configuration only if [Nupf interface settings](#) is selected in the range configuration list.

The following table describes the Slice Mapping settings.

Setting	Description
<i>Slice Mapping:</i>	
	Select the <b>Add Slice Mapping</b> button to add a network slice to your test configuration.
<i>Slice Mapping:</i>	
	Select the <b>Delete Slice Mapping</b> button to remove this network slice from your test configuration.
SST	The Slice/Service Type (SST) value for this network slice.

<b>Setting</b>	<b>Description</b>
SD	The Slice/Service Type (SST) value for this network slice. 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	One or more DNNs (Data Network Names) associated with the network slice and uplink path. Select one or more DNNs from the drop-down list.

## 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:

<b>5G-EIR Ranges panel</b>	<b>558</b>
<b>5G-EIR Range panel</b>	<b>559</b>
<b>5G-EIR Node settings</b>	<b>559</b>
<b>5G-EIR N5g-eir interface settings</b>	<b>560</b>
<b>5G-EIR Remote SBA Nodes</b>	<b>562</b>

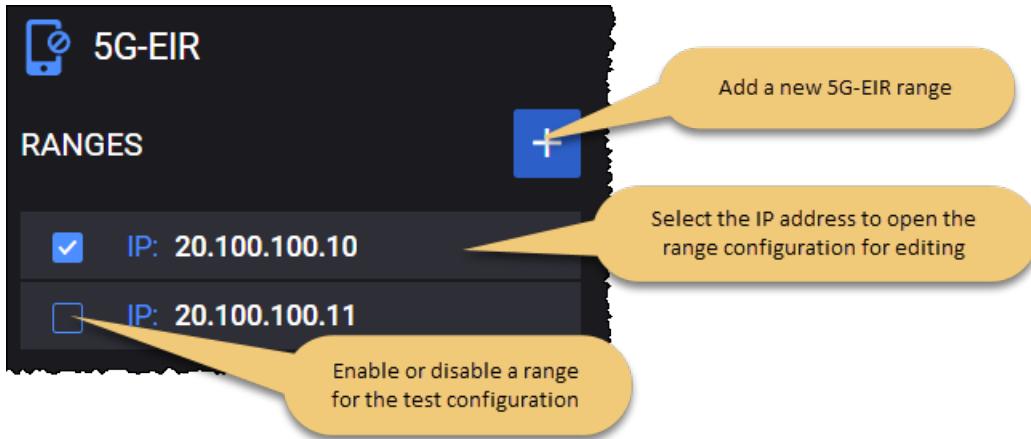
### 5G-EIR Ranges panel

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 ...



If multiple agents are assigned to this node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) displays the available options in the drop-down:

- **One Range on All Agents**
- **Round Robin Ranges on Agents**

**IMPORTANT**

Only one 5G-EIR range can be configured on one agent.

- in case of multiple ranges, it will require one agent for each range;
- in case one range and multiple agents, each agent will create a different 5G-EIR NF, with incremented IP address and NF ID, and whole UE range.

## 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 <b>Delete Range</b> 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 <a href="#">5G-EIR node settings</a> .
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 <a href="#">5G-EIR N5g-eir interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">5G-EIR remote SBA nodes</a> .
DUT N5g-eir IP Address	<div style="background-color: #0070C0; color: white; padding: 2px 5px; margin-right: 10px;"><b>IMPORTANT</b></div> This option appears only if the range is set as DUT. The IP address from your test network to use for traffic on this interface.

## 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	<p>Multiple 5G-EIR instances may be deployed in the 5G network.</p> <p>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.</p>
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
PLMN MCC	<p>The PLMN MCC for this AMF range.</p> <p><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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.

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

## 5G-EIR Remote SBA Nodes

### NRF Connection Settings

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

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

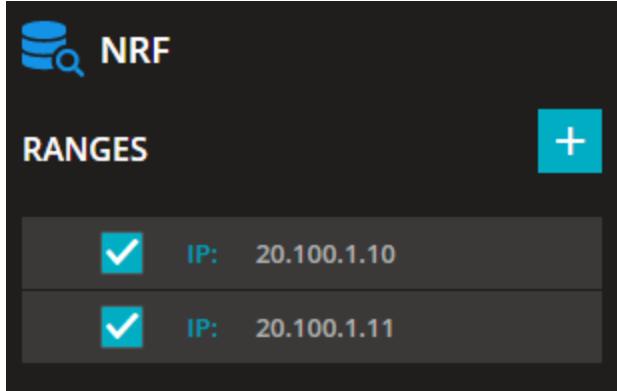
## NF Discovery service

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.

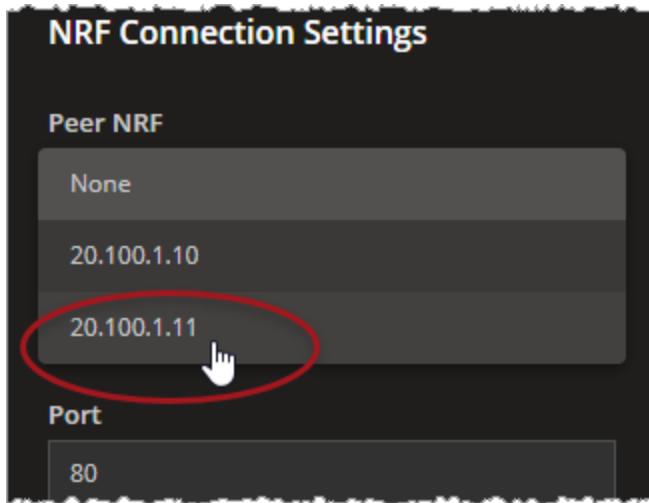
### NF Discovery in LoadCore

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:

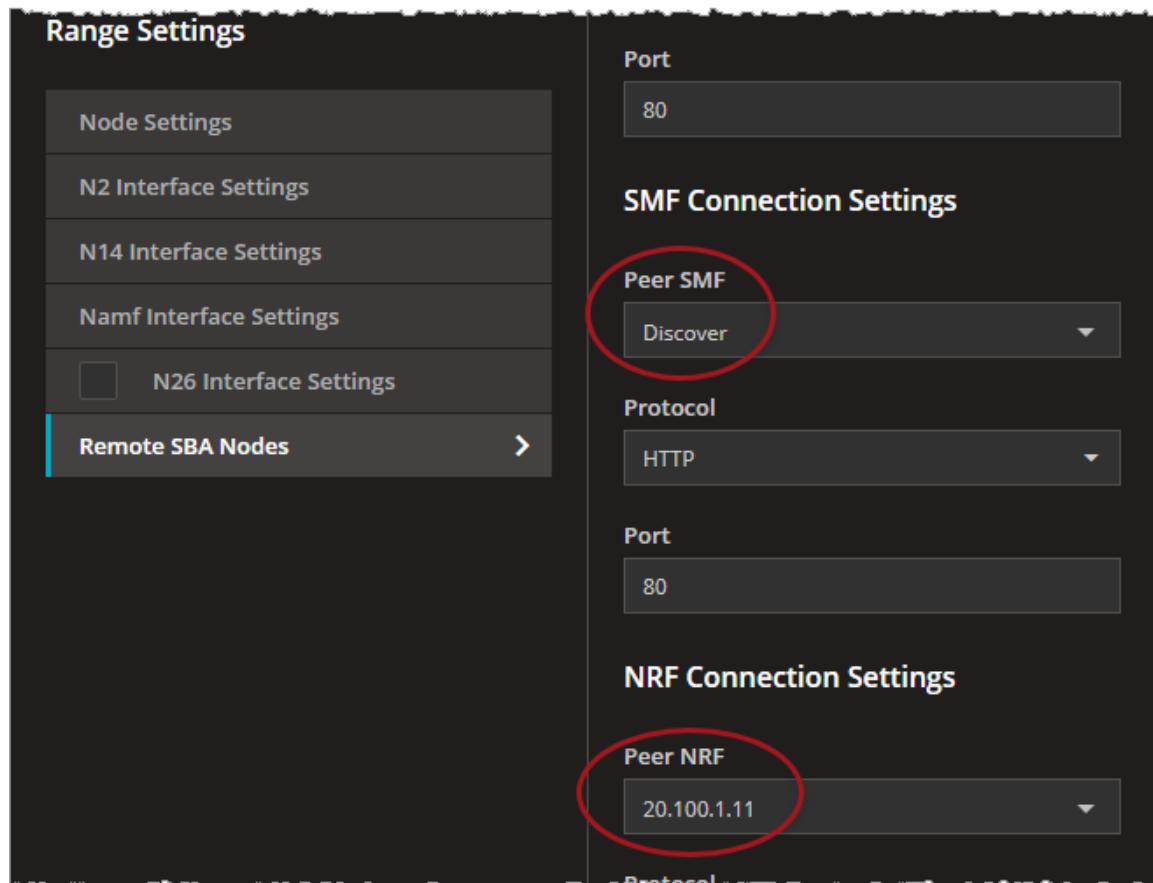


This is the NRF to which the node is registering.

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).

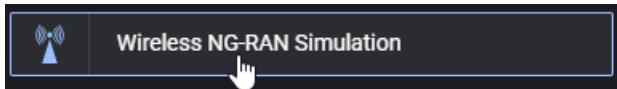
For example:



*CHAPTER 7*

## NG-RAN Simulation tests

This section provides descriptions of the configuration settings that are specific to the **Wireless NG-RAN Simulation** test type.



The NG-RAN simulation test topology is similar to a Full Core test, except that:

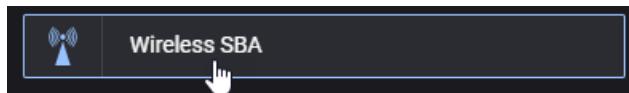
- The AMF and UPF nodes are configured as DUTs.
- The UE, RAN, and DN nodes are enabled for testing.
- All other simulated nodes are disabled by default.

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

*CHAPTER 8*

## SBA tests: configuration settings

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

**Topics:**

<b>SBA Tester overview</b>	<b>570</b>
<b>UE configuration settings</b>	<b>571</b>
UE Ranges panel	572
UE Range panel	572
Range Settings	573
UE Identification	574
UE Security	575
UE Settings	577
UE SDF settings	578
Shared Data IDs	579
UE Subscribed AMBR settings	579
Service Area Restrictions	580
Forbidden Areas	581
Notifications	581
SMS Configuration	582
Network Slicing	584
UDM Default NSSAI settings	585
UDM SNSSAI Mappings	585
UDR SNSSAI Settings	586
Charging Function	587
Converged Charging	587

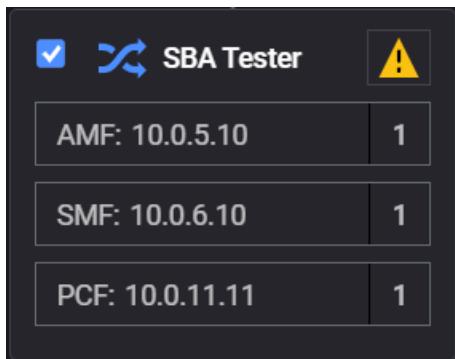
Spending Limit Control .....	588
Objectives .....	591
Primary Objective .....	592
Secondary Objectives .....	631
<b>SBA Tester Global Settings panel .....</b>	<b>658</b>
Connection Settings .....	660
Advanced Settings .....	660
Impairment .....	662
DNNs panel .....	663
DNN configuration settings .....	664
DNN GBR configuration settings .....	665
Session AMBR configuration settings .....	666
QoS Flows panel .....	667
QoS Flow configuration settings .....	668
QoS Flow Packet Filter configuration settings .....	670
QoS Flow Maximum Packet Loss configuration settings .....	671
QoS Flow ARP configuration settings .....	671
QoS Flow MBR configuration settings .....	672
QoS Flow GBR configuration settings .....	672
External Stats Server .....	672
<b>SBA Tester Simulated Nodes panel .....</b>	<b>680</b>
AMF configuration settings .....	680
SMF configuration settings .....	686
PCF configuration settings .....	691
AF configuration settings .....	696
<b>SBA Tester Remote SBA Nodes .....</b>	<b>702</b>
<b>SBA Tester Remote Nodes .....</b>	<b>704</b>
AUSF configuration settings .....	706
AUSF Ranges panel .....	707
AUSF Range panel .....	707
AUSF node settings .....	708
AUSF Nausf interface settings .....	709

AUSF remote SBA nodes .....	710
CHF configuration settings .....	712
CHF Ranges panel .....	712
CHF Range panel .....	713
CHF node settings .....	713
CHF Nchf interface settings .....	714
CHF remote SBA nodes .....	715
NRF configuration settings .....	716
NRF Ranges panel .....	716
NRF Range panel .....	716
NRF node settings .....	717
NRF Nnrf interface settings .....	718
NSSF configuration settings .....	720
NSSF Ranges panel .....	721
NSSF Range panel .....	721
NSSF node settings .....	722
Nnssf Interface Settings .....	723
Remote SBA nodes .....	724
NSSF Restricted NSSAIs .....	725
NSSF Network Slices .....	726
NSSF Configured NSSAI .....	727
PCF configuration settings .....	728
PCF Ranges panel .....	728
PCF Range panel .....	728
PCF node settings .....	729
PCF service area restrictions .....	731
PCF Npcf interface settings .....	732
PCF remote SBA nodes .....	733
SCP configuration settings .....	734
SCP Ranges panel .....	734
SCP Range panel .....	735
SCP Nscp interface settings .....	736

SCP Remote SBA Nodes .....	737
SMSF configuration settings .....	738
SMSF Ranges panel .....	738
SMSF Range panel .....	739
SMSF node settings .....	740
SMSF Nsmsf interface settings .....	740
SMSF Remote SBA Nodes .....	741
UDM configuration settings .....	744
UDM Ranges panel .....	744
UDM Range panel .....	745
UDM node settings .....	746
UDM Nudm interface settings .....	749
UDM remote SBA nodes .....	750
UDR configuration settings .....	751
UDR Ranges panel .....	751
UDR Range panel .....	752
UDR Nudr interface settings .....	754
UDR remote SBA nodes .....	755

## 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:

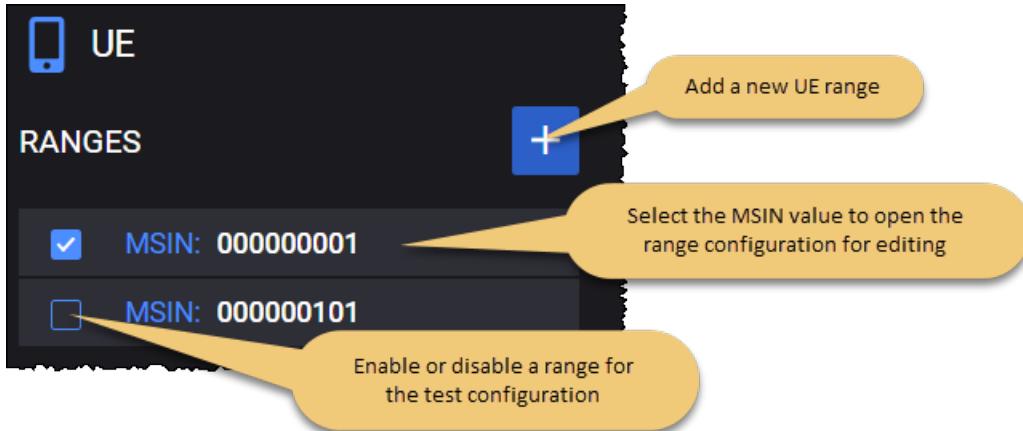
<b>UE Ranges panel</b>	<b>572</b>
<b>UE Range panel</b>	<b>572</b>
<b>Range Settings</b>	<b>573</b>
UE Identification	574
UE Security	575
UE Settings	577
UE SDF settings	578
Shared Data IDs	579
UE Subscribed AMBR settings	579
Service Area Restrictions	580
Forbidden Areas	581
Notifications	581
SMS Configuration	582
<b>Network Slicing</b>	<b>584</b>
UDM Default NSSAI settings	585
UDM SNSSAI Mappings	585
UDR SNSSAI Settings	586
<b>Charging Function</b>	<b>587</b>
Converged Charging	587
Spending Limit Control	588
<b>Objectives</b>	<b>591</b>
Primary Objective	592
Secondary Objectives	631

## 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 <b>Delete Range</b> 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](#)
- [SMS Configuration](#)

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

<b>Setting</b>	<b>Description</b>												
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	The protection scheme used to generate the SUCI (for the purpose of concealing the SUPI) for each UE in the range. The options are as follows: <table border="1" style="margin-left: 20px;"> <thead> <tr> <th><b>Scheme</b></th> <th><b>Identifier</b></th> <th><b>Size of the scheme output</b></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>	<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>	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.
<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>											
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).
<i>Operator Specific Data</i>	
Policy data	This option allows for specific operator data to be added.
Use Operator Specific Data	Enable this option to use operator specific data. A list of objects similar with the reconfigured example is expected.

<b>Setting</b>	<b>Description</b>
Operator Specific Data Policy JSON	<p>Paste the operator specific data in JSON format into the field. Format and save the JSON content by selecting the <b>Save JSON</b> button.</p> <p>Default format:</p> <pre data-bbox="412 407 788 1358"> {     "opSpecDataName1": {         "dataType": "string",         "value": "aaaaaa"     },     "opSpecDataName2": {         "dataType": "object",         "value": {             "member1": 1,             "member2": "string",             "member3": null         }     },     "opSpecDataName3": {         "dataType": "integer",         "value": 1023     },     "opSpecDataName4": {         "dataType": "array",         "value": [             {                 "member1": 1,                 "member2": "string",                 "member3": null             },             1025,             "another string"         ]     } } </pre>

## 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.

<b>Setting</b>	<b>Description</b>
<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

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

## 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 <b>Not Allowed Areas</b> or <b>Allowed Areas</b>.</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
<b>Areas:</b>	
	Select the <b>Add Area</b> button to add a new restriction area to your configuration.
<b>Area:</b>	
	Select the <b>Delete Area</b> 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.
<b>TACs:</b>	
	Select the <b>Add TAC</b> button to add a new TAC to your configuration. Each <b>Area</b> that you add to a UE range's Service Area Restriction contains a

Setting	Description
	<p>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 <b>Delete</b> 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 <b>Delete Forbidden Area</b> 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 <b>Delete</b> button to remove this TAC from your configuration.
TAC	<p>Each <b>Area</b> that you add to a UE range's Forbidden Area contains a list of one or more TACs.</p> <p>A Tracking Area Code (TAC) is a 2 or 3-octet string identifying a Tracking Area within a PLMN. A Tracking Area (TA) is a geographical combination of several neighboring base stations. When a UE is in the Idle state, its location is known to the network at the TA level (versus the cell level, as is the case with a UE in the Connected state). The TAC is used in the construction of the Tracking Area Identity (TAI).</p>

## Notifications

Each UE range in the SBA topology has a set of **Notifications** values that configure Unified Data Repository (UDR) notifications for the range.

The UDR stores policy data that is used by the network service consumers (PCF, UDM, and NEF). Among the functionalities supported by the UDR is subscriptions to notification and the notification of

subscribed data changes.

<b>Setting</b>	<b>Description</b>
<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.

<b>Setting</b>	<b>Description</b>
<i>SMS Configuration:</i>	
SMS Mode	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>SMS-MO:</b> Mobile Originated. The UE range originates (sends) SMS messages.</li> <li>• <b>SMS-MT:</b> Mobile Terminated. The UE range waits for delivery of SMS messages.</li> </ul>
<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"> <li>• Unknown</li> <li>• International number</li> <li>• National number</li> <li>• Network specific number</li> <li>• Subscriber number</li> <li>• Alphanumeric</li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• Abbreviated number</li> <li>• Reserved number</li> </ul>
Numbering Plan Identification	<p>The numbering plan identification can be one of the following:</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• ISDN</li> <li>• Data numbering plan</li> <li>• Telex numbering plan</li> <li>• National numbering plan</li> <li>• Private numbering plan</li> <li>• ERMES numbering plan</li> <li>• Reserved numbering plan</li> </ul>
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.
SMS Management Subscription Data	<p>When selected, this pane displays the following options:</p> <ul style="list-style-type: none"> <li>• <b>Subscribed for MT SMS</b> - by default, this option is enabled.</li> <li>• <b>Barred All MT SMS</b> - by default, this option is disabled.</li> <li>• <b>Barred Roaming MT SMS</b> - by default, this option is disabled.</li> <li>• <b>Subscribed for MO SMS</b> - by default, this option is enabled.</li> <li>• <b>Barred All MO SMS</b> - by default, this option is disabled.</li> <li>• <b>Barred Roaming MO SMS</b> - by default, this option is disabled.</li> </ul> <p>If technical specification Release 16 is configured in <a href="#">Global Settings</a>, the <a href="#">Trace Data</a> option is enabled.</p>
Enable SMS Management Subscription Get	<p>This option has effect only for technical specification Release 16.</p> <p>If active (default), TS 23.502 <i>Registration procedures for SMS over NAS</i> step 7b (<code>Nudm_SDM_Get</code>) is performed.</p>

The following table describes the **Trace Data** settings.

<b>Setting</b>	<b>Description</b>
<i>Trace Data</i>	<i>Select the check box to enable this option.</i>
Trace Reference	The trace reference string should be formed as follows: the concatenation of MCC, MNC and Trace ID as follows: <MCC><MNC><Trace ID>.

Setting	Description
	This field cannot be empty.
Trace Depth	Select an option from the drop-down list: <b>MINIMUM</b> , <b>MEDIUM</b> , <b>MAXIMUM</b> , <b>MINIMUM_WO_VENDOR_EXTENSION</b> , <b>MEDIUM_WO_VENDOR_EXTENSION</b> , <b>MAXIMUM_WO_VENDOR_EXTENSION</b> . Default value: <b>MEDIUM</b> .
NE Types	Configures a hexadecimal number as string, i.e. only values 0-9, a-f are allowed. Default value: <b>000008</b> . This field cannot be empty.
Triggering Events	Configures a hexadecimal number as string, i.e. only values 0-9, a-f are allowed. Default value: <b>0000</b> . This field cannot be empty.
Trace Collection Entity IPv4 Address	Provide the IPv4 address. Default value: <b>192.168.0.1</b> .
Trace Collection Entity IPv6 Address	Provide the IPv6 address. Default value: empty.
List of Interfaces	Configures a hexadecimal number as string, i.e. only values 0-9, a-f are allowed. Can be empty. Default value: empty.

## 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:

<b>UDM Default NSSAI settings</b> .....	<b>585</b>
<b>UDM SNSSAI Mappings</b> .....	<b>585</b>
<b>UDR SNSSAI Settings</b> .....	<b>586</b>

## 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 <b>Add UDM Default NSSAI</b> button to add the default NSSAI to your test configuration.
<i>UDM Default NSSAI settings:</i>	
	Select the <b>Delete UDM Default NSSAI</b> 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 <b>Add SNSSAI Mapping</b> button to add the NSSAI mapping to your test configuration.
<i>UDM SNSSAI Mapping settings:</i>	

Setting	Description
	Select the <b>Delete SNSSAI Mapping</b> 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 <a href="#">DNN configuration settings</a> .

## UDR SNSSAI Settings

The following table describes the UE **UDR SNSSAI** settings.

Setting	Description
<i>UDR SNSSAI Settings:</i>	
	Select the <b>Add SNSSAI Settings</b> button to add the SNSSAI settings to your test configuration.
<i>UDR Settings:</i>	
	Select the <b>Delete SNSSAI Settings</b> 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 <a href="#">DNN configuration settings</a> .

## 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.

<b>Setting</b>	<b>Description</b>
<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.

<b>Setting</b>	<b>Description</b>
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 <a href="#">here</a>.</i>
<i>Notify Policy Counters</i>	<i>These settings are described <a href="#">here</a>.</i>

## Policy Counters

The following table describes the **Policy Counters** settings.

Setting	Description
<i>Policy Counters:</i>	
	Select the <b>Add Policy Counter</b> button to add a policy counter to your test configuration.
<i>Policy Counter settings:</i>	
	Select the <b>Delete Policy Counter</b> 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 <b>Add Pending Status</b> button to add a pending policy counter status.
<i>Pending Policy Counter Status settings:</i>	
	Select the <b>Delete Pending Policy Counter Status</b> 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 <b>Add Policy Counter</b> button to add a policy counter to your test configuration for which you want to receive notifications.

Setting	Description
<i>Policy Counter settings:</i>	
	Select the <b>Delete Policy Counter</b> 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 <b>Add Pending Status</b> button to add a pending policy counter status.
<i>Pending Policy Counter Status settings:</i>	
	Select the <b>Delete Pending Policy Counter Status</b> 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:

<b>Primary Objective</b> .....	<b>592</b>
<b>Secondary Objectives</b> .....	<b>631</b>

## 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>	$20000 / 1000 = 20\text{s}$ 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 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"> <li>• <a href="#">UE Authentication Request AMF to AUSF</a></li> <li>• <a href="#">Create Policy AMF to PCF</a></li> <li>• <a href="#">Create Policy SMF to PCF</a></li> <li>• <a href="#">Initial Spending Limit PCF to CHF</a></li> <li>• <a href="#">Converged Charging SMF to CHF</a></li> <li>• <a href="#">NS Management AMF to NSSF</a></li> <li>• <a href="#">NS Selection Get AMF to NSSF</a></li> <li>• <a href="#">Enable SM Service AMF to SMSF</a></li> </ul>
Objective Type	Select the desired Primary Objective Type: <ul style="list-style-type: none"> <li>• <b>Active Subscribers:</b> 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.</li> <li>• <b>Subscribers Per Second:</b> The test attempts to activate a specified number of subscriber sessions per second, within the rate and time parameters that you configure.</li> </ul> <p>The panel will display the settings for the selected Objective Type.</p>
<i>Active Subscribers:</i>	
Ramp-up Rate	The number of subscriber sessions to activate per second.
Sustain Time	The duration of time (in Seconds) that the specified sessions will remain active.

Parameter	Description
(s)	
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 (s)	The number of seconds that each subscriber session will remain active. This is, therefore, the amount of time that will elapse between the subscriber attach and the subscriber detach. At the end of the session hold time, the subscriber performs the detach procedure.
Rate	The number of subscriber sessions to activate per second.
Sustain Time (s)	The duration of time (in Seconds) that the specified session activation rate will be maintained.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.

### 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).

Procedure setting	Description
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 <b>NR Location</b> to open the configuration panel for these settings, which are described below in <a href="#">User Location</a> .

## 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.

Parameter	Description
<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 <a href="#">DNN configuration settings</a> .
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.

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

## 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.

<b>Parameter</b>	<b>Description</b>
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

Parameter	Description
	specified in TS 23.501, table 5.7.4-1.
ARP:	
ARP Priority Level	<p>Specify the ARP priority level to use for this procedure.</p> <p>The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.</p>
ARP Preemption Capability	<p>Select <b>Not Preemp</b> or <b>May Preempt</b>.</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 <b>Not Preemptable</b> or <b>Preemptable</b>.</p> <p>When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.</p>

## User Location

The User Location values are required by the services that enable an NF to request location information for a target UE. The User Location information includes:

- NR Location: The NR Location values are used in the 5G System by services that track the location of UEs.
- TAI: A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).
- NCGI: In the 5G System, each NR cell is assigned a NR Cell Global Identity (NCGI) value. It is formed by concatenating the PLMN-Id (PLMN Identifier) with the 36-bit NCI (NR Cell Identity).
- 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.

Parameter	Description
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.

### 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.

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

## 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 <b>QoS Settings</b> to open the configuration panel for these settings.</i>	
QoS Settings	
Priority Level	Specify the priority level.
5QI	Specify the 5QI value (decimal number) to use.
ARP	
ARP Priority Level	Specify the ARP priority level. The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by the home network and thus applicable when a UE is roaming.
ARP Preemption Capability	Select <b>Not Preemp</b> or <b>May Preempt</b> . 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 <b>Not Preemptable</b> or <b>Preemptable</b> . 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.
<i>Session AMBR: Select <b>Session AMBR</b> 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	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink

Parameter	Description
Session AMBR Downlink	rate.

## Authorized Settings

These configuration settings are described in the following table.

Parameter	Description
<i>QoS Settings: Select <b>QoS Settings</b> to open the configuration panel for these settings.</i>	
<i>QoS Settings</i>	
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.
5QI	Specify the 5QI value (decimal number) to use.
<i>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>
ARP Preemption Capability	<p>Select <b>Not Preemp</b> or <b>May Preempt</b>.</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 <b>Not Preemptable</b> or <b>Preemptable</b>.</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>

Parameter	Description
<i>Session AMBR: Select <b>Session AMBR</b> 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 <b>NR Location</b> 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.
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.
TAI	
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.
NCGI	
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.
Global Ran Node Id	
MCC	Set the mobile country code.

Parameter	Description
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 <b>EUTRA Location</b> 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.
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.

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.

*N3GA Location:* Select **N3GA Location** to open the configuration panel for these settings.

TAI	
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.
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 <b>Add Group</b> 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.

Parameter	Description
Downlink Volume	Set the total downlink volume value.
Service Specific Units	Set the total service specified units value.
<i>Used Units</i>	
	Select the <b>Add unit</b> 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"> <li>• <b>ONLINE_CHARGING</b></li> <li>• <b>OFFLINE_CHARGING</b></li> </ul>
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"> <li>• <b>INACTIVE</b></li> <li>• <b>ACTIVE</b></li> </ul>
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 <b>QoS Information</b> to open the configuration panel for these settings, which are described below in <a href="#">QoS Information</a> .
<i>Triggers</i>	The Triggers settings are described below in <a href="#">Triggers</a> .

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.
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.
<b>ARP</b>	
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 <b>Not Preemp</b> or <b>May Preempt</b>.</p> <p>When a flow is preemption-vulnerable, it can be dropped to free up</p>

Parameter	Description
	resources for packets that have a higher ARP priority level.
ARP Preemption Vulnerability	Select <b>Not Preemptable</b> or <b>Preemptable</b> . 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.

The following table describes the Triggers settings.

Parameter	Description
	Select the <b>Add Trigger</b> 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: <b>UOTA_THRESHOLD, QHT, FINAL, QUOTA_EXHAUSTED, VALIDITY_TIME, OTHER_QUOTA_TYPE, FORCED_REAUTHORISATION, 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</b>
Trigger Category	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>IMMEDIATE_REPORT</b></li> <li>• <b>DEFERRED_REPORT</b></li> </ul>
Time Limit	Specify the time limit.
Volume Limit 64	Specify the volume limit.
Max Number of ccc	Set the value for this field.

## NS Management AMF to NSSF

The **NS Management AMF to NSSF** 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.

## NS Selection Get AMF to NSSF

The **NS Selection Get AMF to NSSF** Procedure requires the configuration of the *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.

The following table describes the selection settings for the **NS Selection Get AMF to NSSF** procedure.

Parameter	Description
<i>Selection Settings</i>	
TAI	
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>Context Settings</i>	
Context Type	Select an option from the drop-down list: <b>Initial Request</b> or <b>PDU Session Establishment</b> .
Request Mapping	Select the toggle button to enable this option. This option is available only when context type is set to <b>Initial Request</b> .
Subscribed NSAAI	This option is available only when context type is set to <b>Initial Request</b> . Refer to <a href="#">NSSAI</a> settings for details.
Default Subscribed NSAAI	This option is available only when context type is set to <b>Initial Request</b> . Refer to <a href="#">NSSAI</a> settings for details.
Requested NSSAI	This option is available only when context type is set to <b>Initial</b>

Parameter	Description
	<p><b>Request.</b></p> <p>Refer to <a href="#">NSSAI</a> settings for details.</p>
Roaming Indication	<p>Select an option from the drop-down list: <b>NON_ROAMING</b>, <b>LOCAL_BREAKOUT</b>, <b>HOME_ROUTED_ROAMING</b>.</p> <p>This option is available only when context type is set to <b>PDU Session Establishment</b>.</p>
PDU Session S-NSSAI	<p>This option is available only when context type is set to <b>PDU Session Establishment</b>.</p> <p>Refer to <a href="#">S-NSSAI</a> settings for details.</p>

The following table describes the NSSAI settings.

Parameter	Description								
	Select the add button to add the NSSAI settings to your test configuration.								
	Select the delete button to delete the NSSAI settings configuration 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> </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 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 NSSAI.								
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this NSSAI.								

The following table describes the S-NSSAI settings.

Parameter	Description								
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.								

## Enable SM Service AMF to SMSF

The **Enable SM Service AMF to SMSF** procedure requires the *Starting AMF* setting configuration. 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.

The following table describes the configuration settings for the **UE SMS Context Data** procedure.

Parameter	Description
GUAMIs	Select <b>GUAMIs</b> to open the configuration panel for these settings, which are described below in <a href="#">GUAMIs</a> .
Access Type	Select the Access Network type for the policy: <b>3GPP Access</b> or <b>Non-3GPP Access</b> .
User Location Information	Select <b>User Location Information</b> to open the configuration panel for these settings, which are described below in <a href="#">User Location Information</a> .
UE Time Zone	Set the UE time zone.
Trace Data	Select the <b>Trace Data</b> check box to enable this option. The configuration settings are described below in <a href="#">Trace Data</a> .

Parameter	Description
Back-up AMF Info	Select <b>Back-up AMF Info</b> to open the configuration panel for these settings, which are described below in <a href="#">Back-up AMF Info</a> .
UDM Group ID	Set the UDM group ID.
Routing Indicator	Set the routing indicator.

## GUAMIs

These configuration settings are described in the following table.

Parameter	Description
	Select the <b>Add GUAMIs</b> button to add a new GUAMI to your test configuration.
	Select this button to remove the GUAMI from your test configuration.
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.

## User Location Information

These configuration settings are described in the following table.

Parameter	Description
<i>NR Location: Select <b>NR Location</b> 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.
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.

Parameter	Description
<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 <b>EUTRA Location</b> 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.
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>	

Parameter	Description
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 <b>N3GA Location</b> to open the configuration panel for these settings.</i>	
TAI	
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.
UE IPV6 Address	Set the UE IPV6 address.
Port Number	Set the port number.

## Trace Data

These configuration settings are described in the following table.

Parameter	Description
Trace Reference	Set the trace reference value.
Trace Depth	Select the trace Depth from the drop-down list. The available options are: <b>MINIMUM, MEDIUM, MAXIMUM, MINIMUM_WO_VENDOR_EXTENSION, MEDIUM_WO_VENDOR_EXTENSION, MAXIMUM_WO_VENDOR_EXTENSION.</b>
NE types	Set the NE type.
Triggering Events	Specify the triggering events value.
Collection Entity IPv4 Address	Set the IPv4 address.
Collection Entity IPv6 Address	Set the IPv6 address.
List of Interfaces	Specify the list of interfaces.

### Back-up AMF Info

Parameter	Description
	Select the <b>Add Back-up AMF Info</b> button to create a new AMF info back-up.
	Select this button to remove the selected AMF back-up info.
Backup AMF Name	Set the name for the back-up AMF.
<i>GUAMIs</i>	Select <b>GUAMIs</b> to open the configuration panel for these settings, which are described below in <a href="#">GUAMIs</a> .

### SMS Subscription Data AMF to UDM settings

The following table describes the configuration settings for the **SMS Subscription Data AMF to UDM** procedure.

Parameter	Description
<i>SMS Subscription Data AMF to</i>	Select this feature to enable the subscription and retrieval for SMS-data from AMF to UDM

Parameter	Description
<i>UDM</i>	
Enable SMS Subscription Data Flow	If this option is enabled, the AMF will subscribe to UDM for SMS-data. <b>IMPORTANT</b> If the <b>Technical Spec Version</b> is set to <b>R15</b> , then the SMS Data Retrieval procedure will also be performed.
Enable SMS Subscription Data Get	<b>IMPORTANT</b> This option becomes available only if the <b>Enable SMS Subscription Data Flow</b> parameter is enabled, and the <b>Technical Spec Version</b> is set to <b>R16</b> or later. If this option is enabled, the AMF sends a GET request to the resource representing the UE's SMS Subscription Data.

## Policy Authorization AF to PCF

The following table describes the settings for the **Policy Authorization AF to PCF** Procedure.

Procedure setting	Description
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>AF App ID</b></li> <li>• <b>AF Requested Data</b></li> <li>• <b>Media Components</b></li> <li>• <b>Events</b></li> <li>• <b>Subscription Events</b></li> <li>• <b>Delay(s)</b></li> <li>• <b>Send Unsubscribe before Dereistration</b></li> <li>• <b>Send Resource Allocation failure</b></li> <li>• <b>Data to Send for Received Triggers</b></li> <li>• <b>Create SM Policy</b></li> <li>• <b>Delete SM Policy</b></li> <li>• <b>Update SM Policy</b></li> <li>• <b>Select All</b></li> </ul>
AF App ID	The AF application identifier. Default value is UE_IDENTITY.
Media Components	See <a href="#">Media Component</a> table for configuration details.
Events	See <a href="#">Events</a> table for configuration details.
Subscribe	If enabled, it will create a subscription to events for the existing AF application session context. See <a href="#">Subscribe</a> table for configuration details.

<b>Procedure setting</b>	<b>Description</b>
Delay (ms)	Set the delay (in milliseconds) before SMF will trigger SM Policy update procedure after receiving from PCF SM Policy update notify. A 0 value means no delay.
Send Resource Allocation Failure	If enabled, it will configure SMF to reject the creation of resource related to QoS Flows by sending failure code RES_ALLO_FAIL in SM Policy update.
<i>Data to Send for Received Triggers</i>	
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
Trigger Out of Credit Event	<i>If enabled, the SMF will send the NO_CREDIT trigger to PCF and the PCF will notify the AF.</i>
Trigger Type	Select from the drop-down when the SMF node will send the trigger: <ul style="list-style-type: none"> <li>• <b>Flow Information Received</b></li> <li>• <b>Trigger Requested</b></li> </ul>
Final Unit Action	Indicates the termination action to be taken when the user's account cannot cover the service cost. Available options are: <ul style="list-style-type: none"> <li>• <b>TERMINATE</b></li> <li>• <b>REDIRECT</b></li> <li>• <b>RESTRICT_ACCESS</b></li> </ul>
Trigger QoS Monitoring Event	If selected, it enables the QoS monitoring for UL, DL or round trip delay.
Create SM Policy	<i>This option should be enabled in case of simulated SMF, in order to create SM Policy before Policy Authorization Create. See <a href="#">Create SM Policy</a> table for configuration details.</i>
Update SM Policy	<i>This option should be enabled in case of simulated SMF, in order to update SM Policy after Policy Authorization Create. See <a href="#">Update SM Policy</a> table for configuration details.</i>
Delete SM Policy	<i>This option should be enabled in case of simulated SMF, in order to delete SM Policy after Policy Authorization Delete. See <a href="#">Delete SM Policy</a> table for configuration details.</i>

## Media Component

Parameter	Description
	Select the add button to add the media component settings to your test configuration.
<i>Settings:</i>	
	Select the delete button to delete the media component settings configuration from your test configuration.
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Minimum Requested Bandwidth</b></li> <li>• <b>Maximum Requested Bandwidth</b></li> <li>• <b>Maximum Packet Loss Rate</b></li> <li>• <b>Media Type</b></li> <li>• <b>Flow Status</b></li> <li>• <b>Media Subcomponents</b></li> <li>• <b>Select All</b></li> </ul>
<i>Minimum Requested Bandwidth:</i>	
Uplink	Set the minimum uplink bitrate.
Downlink	Set the minimum downlink bitrate.
<i>Maximum Requested Bandwidth:</i>	
Uplink	Set the maximum uplink bitrate.
Downlink	Set the maximum downlink bitrate.
<i>Maximum Packet Loss Rate:</i>	
Uplink	The maximum uplink packet loss rate (packets per second) that is permitted for the QoS Flow.
Downlink	The maximum downlink packet loss rate (packets per second) that is permitted for the QoS Flow.
Media Type	Select the media type of the service. Available options are: <ul style="list-style-type: none"> <li>• <b>AUDIO</b></li> <li>• <b>VIDEO</b></li> <li>• <b>DATA</b></li> <li>• <b>APPLICATION</b></li> <li>• <b>CONTROL</b></li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>TEXT</b></li> <li>• <b>MESSAGE</b></li> <li>• <b>OTHER</b></li> </ul>
Flow Status	Select the the status of the service data flows. Available options are: <ul style="list-style-type: none"> <li>• <b>ENABLED-UPLINK</b></li> <li>• <b>ENABLED-DOWNLINK</b></li> <li>• <b>DATA</b></li> <li>• <b>ENABLED</b></li> <li>• <b>DISABLED</b></li> <li>• <b>REMOVED</b></li> </ul>
<i>Media Subcomponents:</i>	
	Select to add the media subcomponent settings to your test configuration.
	Select to delete the media subcomponent settings configuration from your test configuration.
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Flow Direction</b></li> <li>• <b>Flow Status</b></li> <li>• <b>Flow Usage</b></li> <li>• <b>Transport</b></li> <li>• <b>Select All</b></li> </ul>
Flow Direction	Select from the drop-down list the direction of the data flow on which the filter is applied: <b>Uplink</b> , <b>Downlink</b> , <b>Bidirectional</b> or <b>Unspecified</b> . This parameter is used to create Flow Description.
Flow Status	Select the the status of the service data flows. Available options are: <ul style="list-style-type: none"> <li>• <b>ENABLED-UPLINK</b></li> <li>• <b>ENABLED-DOWNLINK</b></li> <li>• <b>DATA</b></li> <li>• <b>ENABLED</b></li> <li>• <b>DISABLED</b></li> <li>• <b>REMOVED</b></li> </ul>
Flow Usage	Select from the drop-down the flow usage for this flow: <ul style="list-style-type: none"> <li>• <b>NO_INFORMATION</b></li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>RTCP</b></li> <li>• <b>AF_SIGNALLING</b></li> </ul>
<i>Transport:</i>	
Type	Select the transport protocol specification type: <ul style="list-style-type: none"> <li>• <b>Value</b></li> <li>• <b>Keyword</b></li> </ul>
Value	Set a value for the transport type. <ul style="list-style-type: none"> <li>• If <b>Type</b> is set as <b>Value</b>, add an integer between 0 and 254.</li> <li>• If <b>Type</b> is set as <b>Keyword</b>, then the value is a string.</li> </ul>

## Events

Parameter	Description
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
<i>Items:</i>	
	Select to add the item settings to your test configuration.
	Select to delete the item settings configuration from your test configuration.
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
Event	Select from the drop-down the type of events to include in this item. <b>IMPORTANT</b> The option list depends on the <b>Technical Spec Version</b> set in Global Settings.
Notification Method	Select from the drop-down the notification method to use with this event. <b>IMPORTANT</b> The option list depends on the <b>Technical Spec Version</b> set in Global Settings.
Waiting Time (s)	Indicates the minimum waiting time between subsequent reports. <b>IMPORTANT</b> This setting is only visible when Technical Spec Version is set to 15, and Notification Method is set to <i>EVENT_DETECTION</i> .
Report Period (s)	Indicates the time interval between successive event notifications.

Parameter	Description	
	IMPORTANT	This setting is only visible when Technical Spec Version is set to 16 or higher, and Notification Method is set to <i>PERIODIC</i> .
Requested QoS Monitoring Parameter	IMPORTANT	<p>This parameter appears only if <b>Item's Event</b> parameter is set as <i>QOS_Monitoring</i>.</p> <p>Indicates the UL packet delay, DL packet delay and/or round trip packet delay between the UE and the UPF to be monitored. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>DLINK</b></li> <li>• <b>UPLINK</b></li> <li>• <b>ROUND_TRIP</b></li> <li>• <b>Select/Deselect All</b></li> </ul>
<i>QoS Monitoring Information</i>	IMPORTANT	<i>This parameter appears only if Item's Event parameter is set as QOS_Monitoring.</i>
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.	
Downlink Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for DL packet delay.	
Uplink Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for UL packet delay.	
Round Trip Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for round trip packet delay.	

## Subscribe

Parameter	Description	
Send Unsubscribe before Dereistration	If enabled, it will configure the simulated AF to send Unsubscribe request before UE deregisters.	
<i>Subscription Events</i>		
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.	
<i>Items:</i>		
	Select to add the item settings to your test configuration.	

Parameter	Description
	Select to delete the item settings configuration from your test configuration.
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
Event	Select from the drop-down the type of events to include in this item. <b>IMPORTANT</b> The option list depends on the <b>Technical Spec Version</b> set in Global Settings.
Notification Method	Select from the drop-down the notification method to use with this event. <b>IMPORTANT</b> The option list depends on the <b>Technical Spec Version</b> set in Global Settings.
Waiting Time (s)	Indicates the minimum waiting time between subsequent reports. <b>IMPORTANT</b> This setting is only visible when Technical Spec Version is set to 15, and Notification Method is set to <i>EVENT_DETECTION</i> .
Report Period (s)	Indicates the time interval between successive event notifications. <b>IMPORTANT</b> This setting is only visible when Technical Spec Version is set to 16 or higher, and Notification Method is set to <i>PERIODIC</i> .
Requested QoS Monitoring Parameter	<b>IMPORTANT</b> This parameter appears only if <b>Item's Event</b> parameter is set as <i>QOS_Monitoring</i> . Indicates the UL packet delay, DL packet delay and/or round trip packet delay between the UE and the UPF to be monitored. Available options are: <ul style="list-style-type: none"><li>• <b>DOWNLINK</b></li><li>• <b>UPLINK</b></li><li>• <b>ROUND_TRIP</b></li><li>• <b>Select/Deselect All</b></li></ul>
<i>QoS Monitoring Information</i>	<b>IMPORTANT</b> This parameter appears only if <b>Item's Event</b> parameter is set as <i>QOS_Monitoring</i> .
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
Downlink Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for DL packet delay.
Uplink Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for UL packet delay.
Round Trip	Unsigned integer identifying a threshold (in units of milliseconds) for round

Parameter	Description
Threshold	trip packet delay.

## Create SM Policy

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 <a href="#">DNN configuration settings</a> .
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 SST	Specify the Slice/Service Type (SST) 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).
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.

Procedure setting	Description
Subs Session AMBR Downlink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink rate.
Supported Features	Specify the Supported Features attribute for this policy association. This attribute indicates the negotiated supported features for this policy association. It is a hexadecimal string that indicates the features supported (as described in TS 29.571).
<i>QoS Settings</i>	<i>Select to open the configuration panel for these settings, which are described below in <a href="#">QoS Settings</a>.</i>
<i>User Location</i>	<i>Select to open the configuration panel for these settings, which are described below in <a href="#">User Location Information</a>.</i>

## QoS Settings

The Create SM Policy 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 <b>Not Preemp</b> or <b>May Preempt</b> . 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	Select <b>Not Preemptable</b> or <b>Preemptable</b> . When a flow is preemption-capable, it can be allocated resources that were

Parameter	Description
Vulnerability	already assigned to another data flow that has a lower ARP priority level.

## User Location Information

These configuration settings are described in the following table.

Parameter	Description
<i>NR Location: Select <b>NR Location</b> 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.
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.
TAI	
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.
NCGI	
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.
Global Ran Node ID	
MCC	Set the mobile country code.
MNC	Set the mobile network code.
N3 Iwf ID	Set the value for this field.

Parameter	Description
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 <b>EUTRA Location</b> 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.
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.

Parameter	Description
GNB value	Set the GNB value.
Nge Nb ID	Set the value for this field.
<i>N3GA Location: Select <b>N3GA Location</b> to open the configuration panel for these settings.</i>	
TAI	
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.
UE IPV6 Address	Set the UE IPV6 address.
Port Number	Set the port number.

## Update SM Policy

Parameter	Description
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"> <li>• <b>PLMN_CH</b> – PLMN Change</li> <li>• <b>RES_MO_RE</b> – a request for resource modification has been received by the SMF. The SMF always reports to the PCF.</li> <li>• <b>AC_TY_CH</b> – Access Type Change</li> <li>• <b>UE_IP_CH</b> – UE IP address change. The SMF always reports to the PCF.</li> <li>• <b>UE_MAC_CH</b> – a new UE MAC address is detected or a used UE MAC address is inactive for a specific period</li> <li>• <b>AN_CH_COR</b> – Access Network Charging Correlation Information</li> <li>• <b>US_RE</b> – 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.</li> <li>• <b>APP_STA</b> – the start of application traffic has been detected.</li> <li>• <b>APP_STO</b> – the stop of application traffic has been detected.</li> <li>• <b>AN_INFO</b> – Access Network Information report</li> <li>• <b>CM_SES_FAIL</b> – credit management session failure</li> <li>• <b>PS_DA_OFF</b> – the SMF reports when the 3GPP PS Data Off status changes. The SMF always reports to the PCF.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>DEF_QOS_CH</b> – default QoS Change. The SMF always reports to the PCF.</li> <li>• <b>SE_AMBR_CH</b> – session AMBR Change. The SMF always reports to the PCF.</li> <li>• <b>QOS_NOTIF</b> – the SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be guaranteed or guaranteed again.</li> <li>• <b>NO_CREDIT</b> – Out of credit</li> <li>• <b>PRA_CH</b> – change of UE presence in Presence Reporting Area</li> <li>• <b>SAREA_CH</b> – Location Change with respect to the Serving Area</li> <li>• <b>SCNN_CH</b> – Location Change with respect to the Serving CN node</li> <li>• <b>RE_TIMEOUT</b> – indicates the SMF generated the request because there has been a PCC revalidation timeout</li> <li>• <b>RES_RELEASE</b> – indicates that the SMF can inform the PCF of the outcome of the release of resources for those rules that require so.</li> <li>• <b>SUCC_RES_ALLO</b> – indicates that the requested rule data is the successful resource allocation.</li> <li>• <b>RAT_TY_CH</b> – RAT Type Change.</li> <li>• <b>REF_QOS_IND_CH</b> – Reflective QoS indication Change</li> </ul>
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.
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.
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.
UE Time Zone	Set the UE time zone.
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.
Subs Session AMBR Uplink	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Subs Session AMBR	Specify the subscribed session AMBR (Aggregate Maximum Bit Rate) downlink rate.

Parameter	Description
Downlink	
QoS Flow Usage	<p>Available options:</p> <ul style="list-style-type: none"> <li>• <b>GENERAL</b> – indicates that no specific QoS flow usage information is available.</li> <li>• <b>IMS_SIG</b> – indicate that the QoS flow is used for IMS signaling only.</li> </ul>
<i>User Location</i>	
User Location Information	<i>Select to open the configuration panel for these settings, which are described in <a href="#">User Location Information</a>.</i>
QoS Settings	<i>Select to open the configuration panel for these settings, which are described below in <a href="#">QoS Settings</a>.</i>

## Delete SM Policy

Parameter	Description
UE Time Zone	Set the UE time zone.
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.
<i>User Location</i>	
User Location Information	<i>Select to open the configuration panel for these settings, which are described in <a href="#">User Location Information</a>.</i>

## 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

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 <b>Delete Objective</b> 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 <b>Delete Objective</b> 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"> <li>• <b>Initial Registration</b> – executes only when there is no AMF currently registered for the UE (either at start or when deregistered).</li> <li>• <b>Inter AMF Mobility</b> – executes after initial registration and does inter-AMF mobility registration</li> <li>• <b>Initial And Mobility</b> – does both the initial and the mobility AMF registration.</li> </ul>
Next AMF	Describes how the next AMF is selected when doing AMF mobility registration: <ul style="list-style-type: none"> <li>• <b>Next Round Robin</b> – selects the next AMF from the list in round-robin fashion.</li> <li>• <b>Next Random</b> – selects the next AMF from the list randomly.</li> </ul>

## 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 <b>Delete Objective</b> 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 <b>Delete Objective</b> 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 <b>Delete Objective</b> 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 <b>NR Location</b> 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.

<b>Parameter</b>	<b>Description</b>
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 <b>Delete Objective</b> 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 <b>Delete Objective</b> 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"> <li>• <b>PLMN_CH</b> – PLMN Change</li> <li>• <b>RES_MO_RE</b> – a request for resource modification has been received by the SMF. The SMF always reports to the PCF.</li> <li>• <b>AC_TY_CH</b> – Access Type Change</li> <li>• <b>UE_IP_CH</b> – UE IP address change. The SMF always reports to the PCF.</li> <li>• <b>UE_MAC_CH</b> – a new UE MAC address is detected or a used UE MAC address is inactive for a specific period</li> <li>• <b>AN_CH_COR</b> – Access Network Charging Correlation Information</li> <li>• <b>US_RE</b> – 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.</li> <li>• <b>APP_STA</b> – the start of application traffic has been detected.</li> <li>• <b>APP_STO</b> – the stop of application traffic has been detected.</li> <li>• <b>AN_INFO</b> – Access Network Information report</li> <li>• <b>CM_SES_FAIL</b> – credit management session failure</li> <li>• <b>PS_DA_OFF</b> – the SMF reports when the 3GPP PS Data Off status changes. The SMF always reports to the PCF.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>DEF_QOS_CH</b> – default QoS Change. The SMF always reports to the PCF.</li> <li>• <b>SE_AMBR_CH</b> – session AMBR Change. The SMF always reports to the PCF.</li> <li>• <b>QOS_NOTIF</b> – the SMF notify the PCF when receiving notification from RAN that QoS targets of the QoS Flow cannot be guaranteed or guaranteed again.</li> <li>• <b>NO_CREDIT</b> – Out of credit</li> <li>• <b>PRA_CH</b> – change of UE presence in Presence Reporting Area</li> <li>• <b>SAREA_CH</b> – Location Change with respect to the Serving Area</li> <li>• <b>SCNN_CH</b> – Location Change with respect to the Serving CN node</li> <li>• <b>RE_TIMEOUT</b> – indicates the SMF generated the request because there has been a PCC revalidation timeout</li> <li>• <b>RES_RELEASE</b> – indicates that the SMF can inform the PCF of the outcome of the release of resources for those rules that require so.</li> <li>• <b>SUCC_RES_ALLO</b> – indicates that the requested rule data is the successful resource allocation.</li> <li>• <b>RAT_TY_CH</b> – RAT Type Change.</li> <li>• <b>REF_QOS_IND_CH</b> – Reflective QoS indication Change</li> </ul>
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"> <li>• <b>GENERAL</b> – indicates that no specific QoS flow usage information is available.</li> <li>• <b>IMS_SIG</b> – indicate that the QoS flow is used for IMS signaling only.</li> </ul>
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 <b>Delete Objective</b> 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 send.
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 <b>DNN configuration settings</b> .

## DeregistrationSMF2UDM

The following table describes the **Settings** for the *DeregistrationSMF2UDM* Secondary Objective.

Parameter	Description
	Select the <b>Delete Objective</b> 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 <b>Automatic</b> , the secondary objectives will start automatically. When it is set to <b>Manual</b> , 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 <b>Delete Objective</b> 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 <b>Delete Objective</b> 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 <a href="#">below</a>.</i>

## Rating Groups

The following table describes the Rating Groups settings.

Parameter	Description
	Select the <b>Add Group</b> 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 <b>Add unit</b> 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"> <li>• <b>ONLINE_CHARGING</b></li> <li>• <b>OFFLINE_CHARGING</b></li> </ul>
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"> <li>• <b>INACTIVE</b></li> <li>• <b>ACTIVE</b></li> </ul>
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 <b>QoS Information</b> to open the configuration panel for these settings, which are described below in <a href="#">QoS Information</a> .
Triggers	The Triggers settings are described below in <a href="#">Triggers</a> .

## QoS Information

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.
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.
<b>ARP</b>	
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 <b>Not Preemp</b> or <b>May Preempt</b>.</p> <p>When a flow is preemption-vulnerable, it can be dropped to free up</p>

Parameter	Description
	resources for packets that have a higher ARP priority level.
ARP Preemption Vulnerability	Select <b>Not Preemptable</b> or <b>Preemptable</b> . 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 <b>Add Trigger</b> 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: <b>UOTA_THRESHOLD</b> , <b>QHT</b> , <b>FINAL</b> , <b>QUOTA_EXHAUSTED</b> , <b>VALIDITY_TIME</b> , <b>OTHER_QUOTA_TYPE</b> , <b>FORCED_REAUTHORISATION</b> , <b>UNUSED_QUOTA_TIMER</b> , <b>UNIT_COUNT_INACTIVITY_TIMER</b> , <b>ABNORMAL_RELEASE</b> , <b>QOS_CHANGE</b> , <b>VOLUME_LIMIT</b> , <b>TIME_LIMIT</b> , <b>PLMN_CHANGE</b> , <b>USER_LOCATION_CHANGE</b> , <b>RAT_CHANGE</b> , <b>UE_TIMEZONE_CHANGE</b> , <b>TARIFF_TIME_CHANGE</b> , <b>MAX_NUMBER_OF_CHANGES_IN_CHARGING_CONDITIONS</b> , <b>MANAGEMENT_INTERVENTION</b> , <b>CHANGE_OF_UE_PRESENCE_IN_PRESENCE_REPORTING_AREA</b> , <b>CHANGE_OF_3GPP_PS_DATA_OFF_STATUS</b> , <b>SERVING_NODE_CHANGE</b> , <b>REMOVAL_OF_UPF</b> , <b>ADDITION_OF_UPF</b> , <b>START_OF_SERVICE_DATA_FLOW</b>
Trigger Category	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>IMMEDIATE_REPORT</b></li> <li>• <b>DEFERRED_REPORT</b></li> </ul>
Time Limit	Specify the time limit.
Volume Limit 64	Specify the volume limit.
Max Number of ccc	Set the value for this field.

## UplinkSMSAMF2SMSF

The following table describes the **Settings** for the *UplinkSMSAMF2SMSF* Secondary Objective.

Parameter	Description
	Select the <b>Delete Objective</b> button to delete this Secondary Objective from your test configuration.
Procedure	Uplink SMS AMF to SMSF.
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.
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>Uplink SMS AMF to SMSF</i>	
SMS Record Data	The required setting are described <a href="#">below</a> .
SMS Configuration	The required setting are described <a href="#">below</a> .

## SMS Record Data

The following table describes the SMS Record Data settings.

Parameter	Description
Access Type	Select the access type: <b>3GPP ACCESS</b> or <b>NON 3GPP ACCESS</b> .
User Location Information	Select <b>User Location Information</b> to open the configuration panel for these settings, which are described below in <a href="#">User Location Information</a> .
UE Time Zone	Set the UE time zone.

The User Location Information settings are described in the following table.

Parameter	Description
<i>NR Location: Select <b>NR Location</b> 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 <b>EUTRA Location</b> 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 <b>N3GA Location</b> 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.

## SMS Configuration

The following table describes the SMS Configuration settings.

Parameter	Description
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"> <li>• Unknown</li> <li>• International number</li> <li>• National number</li> <li>• Network specific number</li> <li>• Subscriber number</li> <li>• Alphanumeric</li> <li>• Abbreviated number</li> <li>• Reserved number</li> </ul>
Numbering Plan Identification	The numbering plan identification can be one of the following: <ul style="list-style-type: none"> <li>• Unknown</li> <li>• ISDN</li> <li>• Data numbering plan</li> <li>• Telex numbering plan</li> <li>• National numbering plan</li> <li>• Private numbering plan</li> <li>• ERMES numbering plan</li> <li>• Reserved numbering plan</li> </ul>
Character Set	The character set used in the data coding scheme for the text message.
Destination MSISDN	The destination MSISDN for the SMS text message.
Destination MSISDN Increment	The increment for the destination MSISDN.

## PolicyUpdateAF2PCF

The following table describes the **Settings** for the *PolicyUpdateAF2PCF* Secondary Objective.

Parameter	Description
	Select the <b>Delete Objective</b> button to delete this Secondary Objective from your test configuration.
Procedure	Update Policy AF to PCF.
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.
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>Policy Update AF to PCF</i>	
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>AF App ID</b></li> <li>• <b>Media Components</b></li> <li>• <b>Events</b></li> </ul>
Media Components	See <a href="#">Media Component</a> table for configuration details.
Remove Event Subscription	If enabled, it will remove the existing event subscription information from the application session context.
Events	See <a href="#">Events</a> table for configuration details.
<i>User Location:</i>	
NR Location	Select <b>NR Location</b> to open the configuration panel for the User Location settings (described below).

## Media Component

Parameter	Description
	Select the add button to add the media component settings to your test configuration.

Parameter	Description
<i>Media Component:</i>	
	Select the delete button to delete the media component settings configuration from your test configuration.
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Media Component</b></li> </ul>
Media Component Number	Identifies the media component number, and it contains the ordinal number of the media component.
Null Media Component	If enabled, it will remove the Media Component information from the application session context.
Media Component	<i>Select to open the configuration panel.</i>
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Minimum Requested Bandwidth</b></li> <li>• <b>Maximum Requested Bandwidth</b></li> <li>• <b>Maximum Packet Loss Rate</b></li> <li>• <b>Media Type</b></li> <li>• <b>Flow Status</b></li> <li>• <b>Media Subcomponents</b></li> <li>• <b>Select All</b></li> </ul>
<i>Minimum Requested Bandwidth:</i>	
Uplink	Set the minimum uplink bitrate.
Downlink	Set the minimum downlink bitrate.
<i>Maximum Requested Bandwidth:</i>	
Uplink	Set the maximum uplink bitrate.
Downlink	Set the maximum downlink bitrate.
<i>Maximum Packet Loss Rate:</i>	
Uplink	The maximum uplink packet loss rate (packets per second) that is permitted for the QoS Flow.
Downlink	The maximum downlink packet loss rate (packets per second) that is permitted

Parameter	Description
	for the QoS Flow.
Media Type	Select the media type of the service. Available options are: <ul style="list-style-type: none"> <li>• <b>AUDIO</b></li> <li>• <b>VIDEO</b></li> <li>• <b>DATA</b></li> <li>• <b>APPLICATION</b></li> <li>• <b>CONTROL</b></li> <li>• <b>TEXT</b></li> <li>• <b>MESSAGE</b></li> <li>• <b>OTHER</b></li> </ul>
Flow Status	Select the the status of the service data flows. Available options are: <ul style="list-style-type: none"> <li>• <b>ENABLED-UPLINK</b></li> <li>• <b>ENABLED-DOWNLINK</b></li> <li>• <b>DATA</b></li> <li>• <b>ENABLED</b></li> <li>• <b>DISABLED</b></li> <li>• <b>REMOVED</b></li> </ul>
<i>Media Subcomponents:</i>	
	Select to add the media subcomponent settings to your test configuration.
	Select to delete the media subcomponent settings configuration from your test configuration.
<i>Settings:</i>	
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Media Subcomponent</b></li> </ul>
Null Media Subcomponent	If enabled, it will remove the Media Subcomponent information from the application session context.
<i>Media Subcomponents</i>	
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure. The following options are available: <ul style="list-style-type: none"> <li>• <b>Flow Direction</b></li> <li>• <b>Flow Status</b></li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>Flow Usage</b></li> <li>• <b>Transport</b></li> <li>• <b>Select All</b></li> </ul>
Flow Direction	<p>Select from the drop-down list the direction of the data flow on which the filter is applied: <b>Uplink</b>, <b>Downlink</b>, <b>Bidirectional</b> or <b>Unspecified</b>. This parameter is used to create Flow Description.</p>
Flow Status	<p>Select the the status of the service data flows. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>ENABLED-UPLINK</b></li> <li>• <b>ENABLED-DOWNLINK</b></li> <li>• <b>DATA</b></li> <li>• <b>ENABLED</b></li> <li>• <b>DISABLED</b></li> <li>• <b>REMOVED</b></li> </ul>
Flow Usage	<p>Select from the drop-down the flow usage for this flow:</p> <ul style="list-style-type: none"> <li>• <b>NO_INFORMATION</b></li> <li>• <b>RTCP</b></li> <li>• <b>AF_SIGNALLING</b></li> </ul>
<i>Transport:</i>	
Type	<p>Select the transport protocol specification type:</p> <ul style="list-style-type: none"> <li>• <b>Value</b></li> <li>• <b>Keyword</b></li> </ul>
Value	<p>Set a value for the transport type.</p> <ul style="list-style-type: none"> <li>• If <b>Type</b> is set as <b>Value</b>, add an integer between 0 and 254.</li> <li>• If <b>Type</b> is set as <b>Keyword</b>, then the value is a string.</li> </ul>

## Events

Parameter	Description
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
<i>Items:</i>	
	Select to add the item settings to your test configuration.

Parameter	Description
	Select to delete the item settings configuration from your test configuration.
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
Event	Select from the drop-down the type of events to include in this item. <b>IMPORTANT</b> The option list depends on the <b>Technical Spec Version</b> set in Global Settings.
Notification Method	Select from the drop-down the notification method to use with this event. <b>IMPORTANT</b> The option list depends on the <b>Technical Spec Version</b> set in Global Settings.
Waiting Time (s)	Indicates the minimum waiting time between subsequent reports. <b>IMPORTANT</b> This setting is only visible when Technical Spec Version is set to 15, and Notification Method is set to <i>EVENT_DETECTION</i> .
Report Period (s)	Indicates the time interval between successive event notifications. <b>IMPORTANT</b> This setting is only visible when Technical Spec Version is set to 16 or higher, and Notification Method is set to <i>PERIODIC</i> .
Requested QoS Monitoring Parameter	<b>IMPORTANT</b> This parameter appears only if <b>Item's Event</b> parameter is set as <i>QOS_Monitoring</i> . Indicates the UL packet delay, DL packet delay and/or round trip packet delay between the UE and the UPF to be monitored. Available options are: <ul style="list-style-type: none"><li>• <b>DOWNLINK</b></li><li>• <b>UPLINK</b></li><li>• <b>ROUND_TRIP</b></li><li>• <b>Select/Deselect All</b></li></ul>
Null QoS Monitoring Information	If enabled, it will remove the QoS Monitoring Information from the application session context.
<i>QoS Monitoring Information</i>	<b>IMPORTANT</b> <i>This parameter appears only if Item's Event parameter is set as QOS_Monitoring.</i>
Fields to Include in Requests	Select which parameters should be included in the requests sent as part of the Policy Authorization procedure.
Downlink Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for DL packet delay.

Parameter	Description
Uplink Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for UL packet delay.
Round Trip Threshold	Unsigned integer identifying a threshold (in units of milliseconds) for round trip packet delay.

## User Location

The User Location values are required by the services that enable an NF to request location information for a target UE. The User Location information includes:

- NR Location: The NR Location values are used in the 5G System by services that track the location of UEs.
- TAI: A Tracking Area identity (TAI) uniquely identifies a tracking area. It is constructed from the MCC (Mobile Country Code), MNC (Mobile Network Code), and TAC (Tracking Area Code).
- NCGI: In the 5G System, each NR cell is assigned a NR Cell Global Identity (NCGI) value. It is formed by concatenating the PLMN-Id (PLMN Identifier) with the 36-bit NCI (NR Cell Identity).

These configuration settings are described in the following table.

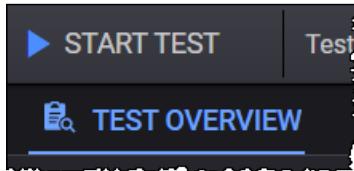
Parameter	Description
<i>NR Location:</i>	
Age of Location information	The Age of Location Information value, at the start of the procedure. The value represents the elapsed time in minutes since the last network contact of the mobile station.
Geographical information	The Geographical Location value that the procedure will use in the identification of the UE location.
Geodetic information	The Geodetic Location value that the procedure will use in the identification of the UE location.
<i>TAI:</i>	
MCC	The PLMN MCC that is used in the construction of this TAI.
MNC	The PLMN MNC that is used in the construction of this TAI.
TAC	The PLMN TAC that is used in the construction of this TAI.
<i>NCGI:</i>	
MCC	The PLMN MCC that is used in the construction of this NCGI.
MNC	The PLMN MNC that is used in the construction of this NCGI.
NR Cell ID	The NCI that is used in the construction of this NCGI.

## 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:

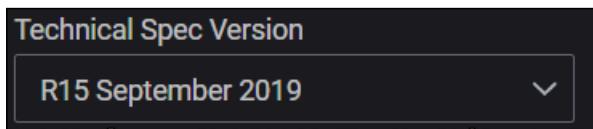


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



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:

<b>Connection Settings</b>	660
<b>Advanced Settings</b>	660
<b>Impairment</b>	662
<b>DNNs panel</b>	663
DNN configuration settings	664
DNN GBR configuration settings	665
Session AMBR configuration settings	666
<b>QoS Flows panel</b>	667
QoS Flow configuration settings	668
QoS Flow Packet Filter configuration settings	670
QoS Flow Maximum Packet Loss configuration settings	671
QoS Flow ARP configuration settings	671
QoS Flow MBR configuration settings	672
QoS Flow GBR configuration settings	672

<b>External Stats Server .....</b>	<b>672</b>
------------------------------------	------------

## 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	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size	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.
Power Saver on Agents	Select this option to disable the IxStack/DPDK at the end of each test on all agents.
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 (sec)	This option becomes available only when <i>Automated Polling Interval</i> option is disabled. It allows you to create a custom polling interval.
Log Level	Select one of the options: <ul style="list-style-type: none"> <li>• <b>Info</b> - Designates informational messages that highlight the progress of the</li> </ul>

Setting	Description
	<p>application at coarse-grained level.</p> <ul style="list-style-type: none"> <li>• <b>Debug</b> - Designates fine-grained informational events that are most useful to debug the application.</li> </ul>
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.

## 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 <b>Add impairment profile</b> button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete impairment profile</b> 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"> <li>• Custom script</li> <li>• PFCP-drop message</li> </ul>
Script file	This parameter is available only when <b>Action Type</b> is set to <b>Custom script</b> . It allows you to add a custom script, using the <b>Upload</b> button. To remove the script, select the <b>Clear</b> 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:

<b>DNN configuration settings</b>	.....	<b>664</b>
<b>DNN GBR configuration settings</b>	.....	<b>665</b>
<b>Session AMBR configuration settings</b>	.....	<b>666</b>

## 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 <b>Delete DNN</b> 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"> <li>• A mandatory Network Identifier that defines the external network to which the UPF is connected.</li> <li>• An optional Operator Identifier that defines the PLMN backbone in which the UPF is located.</li> </ul> <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"> <li>• <b>SSC Mode 1:</b> The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved.</li> <li>• <b>SSC Mode 2:</b> 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.</li> <li>• <b>SSC Mode 3:</b> 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.</li> </ul>
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	Select the desired Subscription Category for this range of UEs. 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).
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.
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 <a href="#">DNN GBR configuration settings</a> .
Session AMBR	Select this option to open a new panel that contains the Session AMBR settings. These settings are described in <a href="#">Session AMBR configuration settings</a> .

## 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	The guaranteed bit rate (bps) for downlink traffic. This is the downlink bit rate

<b>Setting</b>	<b>Description</b>
Rate Downlink	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.

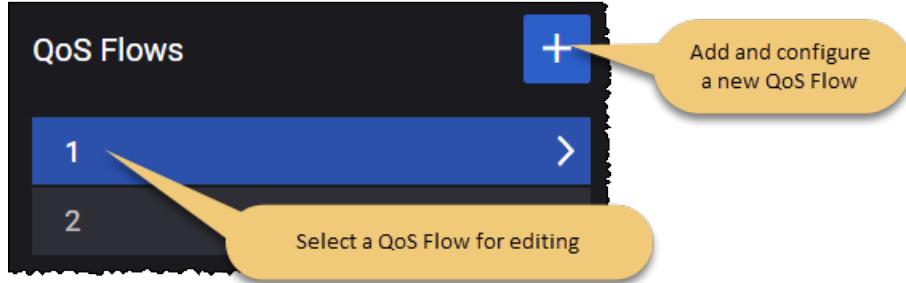
<b>Parameter</b>	<b>Description</b>
Session AMBR Uplink	Specify the DNN session AMBR (Aggregate Maximum Bit Rate) uplink rate.
Session AMBR Uplink Unit	The unit in which the rate is expressed. The options range from bps to Tbps.
Session AMBR Downlink	Specify the DNN session AMBR (Aggregate Maximum Bit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

<b>QoS Flow configuration settings</b>	<b>668</b>
<b>QoS Flow Packet Filter configuration settings</b>	<b>670</b>
<b>QoS Flow Maximum Packet Loss configuration settings</b>	<b>671</b>
<b>QoS Flow ARP configuration settings</b>	<b>671</b>
<b>QoS Flow MBR configuration settings</b>	<b>672</b>
<b>QoS Flow GBR configuration settings</b>	<b>672</b>

## 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.

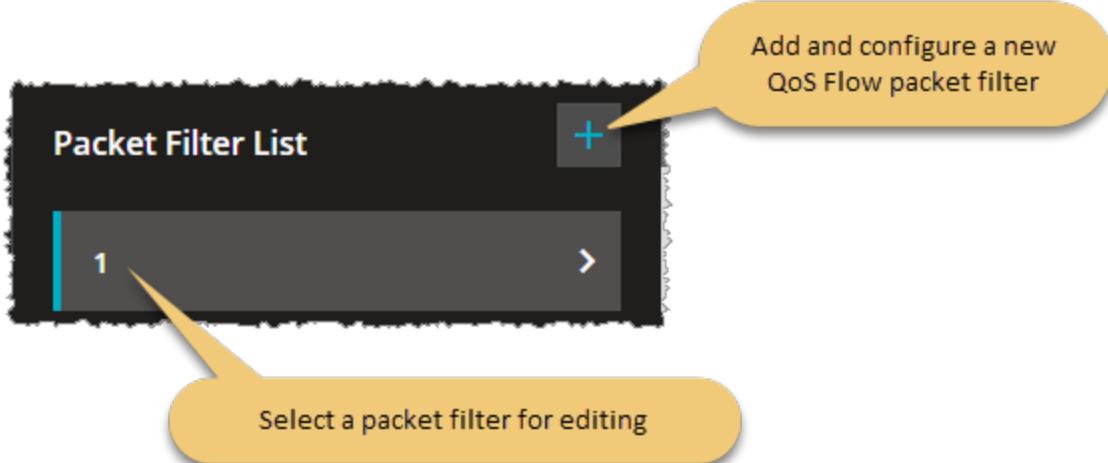
Setting	Description
<i>QoS Flow:</i>	
Is Default	<p>Enable this option if this QoS Flow is associated with the default QoS rule. In the 5G System, a default QoS rule is required for each UE session, and this rule will be associated with a QoS Flow.</p> <p>If this option is not selected, LoadCore makes the <b>Packet Filter List</b> settings available for configuration (refer to <a href="#">QoS Flow Packet Filter configuration settings</a> 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 (non-GBR), 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>

<b>Setting</b>	<b>Description</b>
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><b>IMPORTANT</b> This is available if <a href="#">Is Default</a> option is not selected.</p> <p>Refer to the following topic for a description of the Packet Filter configuration settings: <a href="#">QoS Flow Packet Filter configuration settings</a>.</p>
Max Packet Loss Rate	<p>Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: <a href="#">QoS Flow Maximum Packet Loss configuration settings</a>.</p>
ARP	<p>Refer to the following topic for a description of the ARP configuration settings: <a href="#">QoS Flow ARP configuration settings</a>.</p>
MBR	<p>Refer to the following topic for a description of the MBR configuration settings: <a href="#">QoS Flow MBR configuration settings</a>.</p>
GBR	<p>Refer to the following topic for a description of the GBR configuration settings: <a href="#">QoS Flow GBR configuration settings</a>.</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 <b>Delete Packet Filter</b> 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 setting establish the uplink and downlink maximum packet loss that is permitted for the QoS flow.

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

## QoS Flow ARP configuration settings

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

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

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

## QoS Flow GBR configuration settings

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

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

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

## External Stats Server

If this option is selected, it will allow you to add an external statistic server.

The following table describes the settings required for the External Stats Server configuration.

<b>Setting</b>	<b>Description</b>
<i>External Stats Server:</i>	
Profile	This parameter allows you to upload or remove a stats server profile. Press <b>Upload</b> and load the preferred server profile, or <b>Clear</b> to dismiss one that is set.
Server Address	The address of the external stats server.

## Setting up a Profile

The External Stats Server feature allows you to forward statistic logs to an external server, thus requiring to upload a profile that defines where the stats are stored and what stats should be transferred.

**IMPORTANT** This feature is designed to support any type of external entity, but currently it supports only the Apache Kafka Plugin.

The parameters required to create the request to the external entity are configured in the **Profile** JSON file that is uploaded to Keysight Open RAN Simulators, Cloud Edition 5.1. The following structure and parameters describe the standard content of the JSON file:

<b>Section/ Parameter</b>	<b>Definition</b>	<b>Code Sample</b>
<i>Input section</i>	<i>Lists all the stats/config parameters used in the profile. All the parameters are already available in Keysight Open RAN Simulators, Cloud Edition 5.1. the following types are supported:</i>	
stat	<p>It can be any stat supported in Keysight Open RAN Simulators, Cloud Edition 5.1. The stats can be filtered by any other stat from the stat response.</p>	<p>With filter sample:</p> <pre>{   "type": "stat",   "group": "AgentStatistics",   "stat": "CPU Percent",   "name": "cpu_percent1",   "filterBy": {     "stat": "agentIP",     "value": "10.38.158.83"   } }</pre> <p>Without filter sample:</p> <pre>{   "type": "stat",   "group": "Fullcoreoverview_</pre>

Section/ Parameter	Definition	Code Sample
		<pre>RegisteredAttachedUE",   "stat": "UEs Registered",   "name": "no_of_UE_Registered" }</pre>
config	<p>It can be any parameter exposed in the UI. The path is the same as the one used by the UI to set/get a parameter (see <a href="#">Parameter sample path below</a> image).</p>	<pre>{   "type": "config",   "group": "config/nodes/ausf/ranges/1/nodeSettings",   "stat": "mcc",   "name": "mcc" }</pre>
<i>Mappings section</i>		<p><i>Mapping will use any input parameter referred by name. Mapping also supports mathematical expressions to combine stats.</i></p>
	<p>For example, Keysight Open RAN Simulators, Cloud Edition 5.1 exposes <code>stat1</code> and <code>stat2</code> but the user needs <code>user_stat</code> which comprises <math>(\text{stat1} + \text{stat2}) / 100</math>. The expression is evaluated and the result sent under <code>user_stat</code> name.</p>	<ul style="list-style-type: none"> <li>one parameter sample:</li> </ul> <pre>{   "type": "controlplane",   "from": "no_of_UE_Registered",   "to": "no_of_UE_Registered" }</pre> <p>OR</p> <pre>{   "type": "controlplane",   "from": "mcc",   "to": "MCC" }</pre> <ul style="list-style-type: none"> <li>with mathematical expression:</li> </ul> <pre>{   "type": "controlplane",   "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",   "to": "agent1 cpu ratio" }</pre>

### Parameter sample path

```
{
  "instanceId": "7ea3abc7-f0f6-435b-9154-125deddd101b",
  "mcc": "226",
  "mnc": "04",
  "routingIndicators": [
    1234,
    2222
  ],
  "links": [
    {
      "rel": "self",
      "type": "self",
      "method": "GET",
      "href": "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings"
    },
    {
      "rel": "meta",
      "type": "meta",
      "method": "GET",
      "href": "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings/$options"
    }
  ]
}
```

## Sample profile

```
{
  "profile": {
    "type": "kafka",
    "3gpp_scenario": "QUIC_ABR_DEBUG",
    "event_type": "ATTS_TOOLS_KEYSIGHT_EVENT",
    "specversion": "1.1",
    "kafkatopics": "com.att.ant.stage.ATTSSKeysight.1.0",
    "kafkaschemaUrl": "https%3A%2F%2Fc1001.eastus2.uat.iebus.3pc.att.com%3A8082%2Fschemas%2Fids%2F6635&schemaId=14260",
    "kafkaHeaderBootstrapUrl": "c1001.eastus2.uat.iebus.3pc.att.com:9093",
    "kafkaHeaderSaslMechanism": "PLAIN",
    "kafkaHeaderOAuthScope": "ANT-data-feed-dev-stage",
    "kafkaUsername": "m30317@ant.att.com",
    "kafkaPassword": "August2023#",
    "input": [
      {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent1",
        "filterBy": {
          "stat": "agentIP",
          "value": "10.38.158.83"
        }
      },
      {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent2",
        "filterBy": {
          "stat": "agentIP",
          "value": "10.38.158.83"
        }
      }
    ]
  }
}
```

```

        "value": "10.38.157.97"
    },
},
{
    "type": "config",
    "group": "config/nodes/ausf/ranges/1/nodeSettings",
    "stat": "mcc",
    "name": "mcc"
},
{
    "type": "config",
    "group":
"config/nodes/ue/ranges/1/userPlane/tigerObjective/1/statelessUDP",
    "stat": "ipAddress",
    "name": "ipAddress"
},
{
    "type": "stat",
    "group": "Fullcoreoverview_RegisteredAttachedUE",
    "stat": "UEs Registered",
    "name": "no_of_UE_Registered"
},
{
    "type": "stat",
    "group": "Fullcoreoverview_PDUSessionEstablishment",
    "stat": "PDU Session Establishment Succeeded",
    "name": "no_of_PDU_Session_Established"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
    "stat": "L2-3 Device Rx Traffic",
    "name": "L3 Server::Total Bits/Sec"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
    "stat": "L2-3 Device Tx Traffic",
    "name": "L3 Client::Total Bits/Sec"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_TCPConnections",
    "stat": "TCP connections established",
    "name": "HTTP/s Handshakes Succeeded"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_TCPConnections",
    "stat": "TCP connect failed",
    "name": "HTTP/s Handshakes Failed"
}

```

```

},
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_TCPConnections",
  "stat": "TCP connections closed normally",
  "name": "HTTP/s Connection Closed"
}
],
"mappings": [
  {
    "type": "controlplane",
    "from": "cpu_percent1 + cpu_percent2",
    "to": "total cpu_percent %"
  },
  {
    "type": "controlplane",
    "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",
    "to": "agent1 cpu ratio"
  },
  {
    "type": "controlplane",
    "from": "cpu_percent2/(cpu_percent1 + cpu_percent2)",
    "to": "agent2 cpu ratio"
  },
  {
    "type": "controlplane",
    "from": "mcc",
    "to": "MCC"
  },
  {
    "type": "controlplane",
    "from": "ipAddress",
    "to": "Destination IP Address"
  },
  {
    "type": "controlplane",
    "from": "no_of_UE_Registered",
    "to": "no_of_UE_Registered"
  },
  {
    "type": "controlplane",
    "from": "no_of_PDU_Session_Established",
    "to": "no_of_PDU_Session_Established"
  },
  {
    "type": "userplane",
    "from": "L3 Server::Total Bits/Sec",
    "to": "L3 Server::Total Bits/Sec"
  },
  {
    "type": "userplane",
    "from": "L3 Server::Total Bits/Sec"
  }
]

```

```

        "from": "L3 Client::Total Bits/Sec",
        "to": "L3 Client::Total Bits/Sec"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Handshakes Succeeded",
        "to": "HTTP/s Handshakes Succeeded"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Handshakes Failed",
        "to": "HTTP/s Handshakes Failed"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Connection Closed",
        "to": "HTTP/s Connection Closed"
    }
]
}
}

```

### Event body sent to Kafka

```

[
  {
    "eventBody": {
      "id": "wireless-0acbc45b-8777-4250-a3ec-4f00e47399c8_39",
      "time": "2024-02-29T13:57:35Z",
      "type": "ATTS-TOOLS-KEYSIGHT-EVENT",
      "specversion": "1.1",
      "source": "https://10.38.157.61/wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
      "datacontenttype": "application/json",
      "payload": [
        {
          "type": "resource_info",
          "resource_info": {
            "simulated_tool_info": [
              {
                "tool_name": "LoadCore",
                "middleware_ip": "10.38.157.61"
              }
            ],
            "network_type": "5G",
            "3gpp_scenario": "QUIC_ABR_DEBUG"
          }
        },
        {
          "type": "test_execution_result",
        }
      ]
    }
  }
]
```

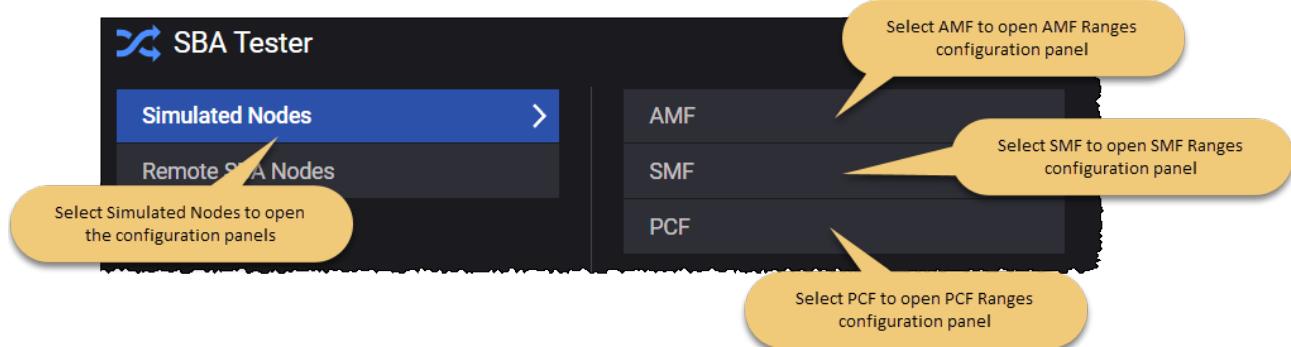
```
        "test_execution_result": {
            "control_plane_result": {
                "Destination IP Address": "20.0.6.10",
                "MCC": "226",
                "agent1 cpu ratio": "0.455321",
                "agent2 cpu ratio": "0.544679",
                "no_of_PDU_Session_Established": "100",
                "no_of_UE_Registered": "0",
                "total cpu_percent %": "3.0902"
            },
            "userplane_plane_result": {
                "L3 Client::Total Bits/Sec": "0",
                "L3 Server::Total Bits/Sec": "0"
            }
        },
        {
            "type": "test_execution_details",
            "test_execution_details": {
                "testName": "4 - Full Core Base Config",
                "testSessionID": "wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
                "UserID": "admin@example.org",
                "testStatus": "STOPPING",
                "testStartTime": "2024-02-29T13:55:40Z",
                "testDuration": 105,
                "testStopTime": "2024-02-29T13:57:31Z"
            }
        }
    ],
    "payloadType": "JSON",
    "value": {}
}
]
```

## 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, PCF or AF range to your test configuration.
- Open an AMF, SMF, PCF or AF 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/AF test configuration Settings. Each range can be accessed and configured by selecting it.



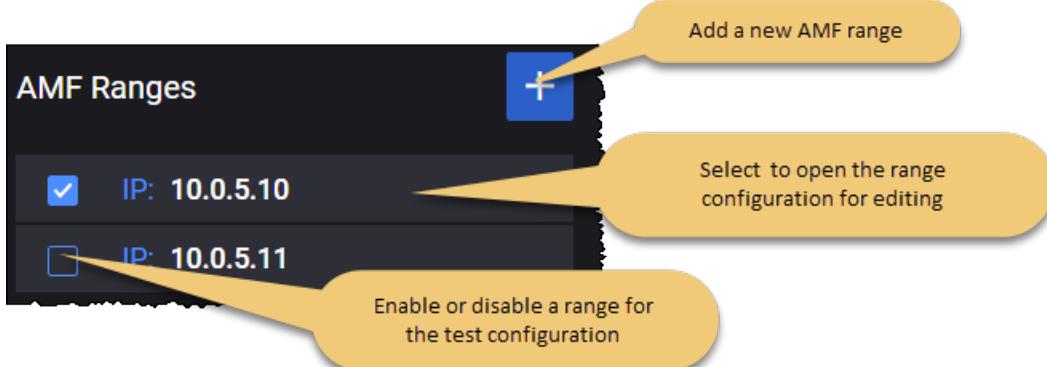
## AMF configuration settings

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.

<b>Setting</b>	<b>Description</b>
<i>AMF:</i>	
	Select the <b>Delete Range</b> 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 <a href="#">AMF Namf interface settings</a> 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.
PLMN MCC	<p>The PLMN MCC for this AMF range.</p> <p><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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>

<b>Setting</b>	<b>Description</b>
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 (ms)	Set the value for the subscription duration.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
Indirect Communication without Delegated Discovery	This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a> .
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, SMSF) for Indirect Communication via SCP.
Indirect Communication with Delegated Discovery	This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a> .
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 (UDM, AUSF, PCF, NSSF, SMSF).
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 <a href="#">Optional Discovery Parameters</a>.</p>

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

<b>Setting</b>	<b>Description</b>
<i>Target Nodes</i>	

<b>Setting</b>	<b>Description</b>
	Select this button to add the a target node to your test configuration.
<i>Settings</i>	
<i>Target Node</i>	
	Select the <b>Delete Target Node</b> 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"> <li>• <b>SUBSCRIPTION</b></li> <li>• <b>POLICY</b></li> <li>• <b>EXPOSURE</b></li> <li>• <b>APPLICATION</b></li> </ul>
<i>Amf Region Id</i>	Set the value for this field.
<i>Network Instance Format</i>	Select the encoding format for the network instance: string or label-list.
<i>Target Nf Fqdn</i>	Set the value for this field.
<i>Pgw</i>	Set the value for this field.
<i>Amf Set Id</i>	Set the value for this field.
<i>Smf Serving Area</i>	Set the value for this field.

<b>Setting</b>	<b>Description</b>
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 <b>Delete Target Plmn</b> 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.
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner</i></p>

Connectivity Settings	Description
	VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.

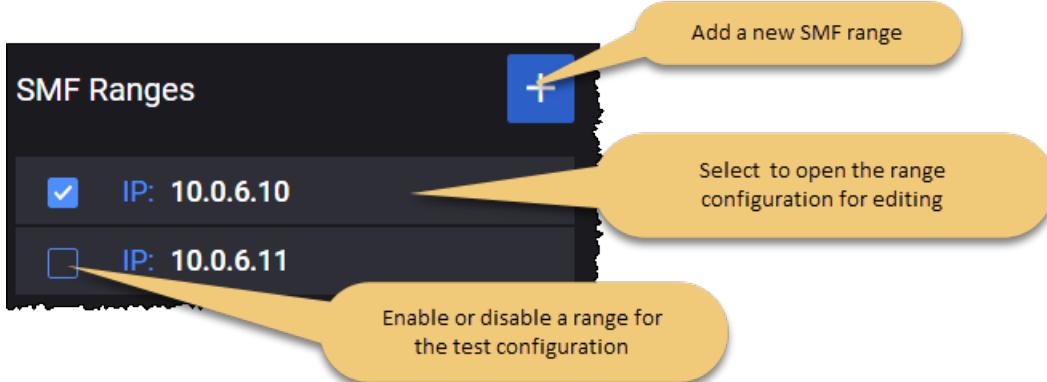
## SMF configuration settings

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
<b>SMF:</b>	
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
<b>Nsmf Interface Settings:</b>	
Connectivity Settings	Each SMF range requires the configuration of Nsmf interface settings. These settings are described below in the <a href="#">SMF Nsmf interface settings</a> section.
<b>Node Settings:</b>	
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.

<b>Setting</b>	<b>Description</b>
PLMN MCC	<p>The PLMN MCC for this AMF range.</p> <p><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	<p>User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.</p>
Indirect Communication without Delegated Discovery	<p>This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a>.</p>
Target Nodes	<p>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.</p>
Indirect Communication with Delegated Discovery	<p>This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a>.</p>
Target Nodes for Delegated Discovery	<p>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.</p>
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 <a href="#">Optional Discovery</a>.</p>

<b>Setting</b>	<b>Description</b>
	<a href="#"><u>Parameters.</u></a>
<i>SMF NSSAI:</i>	
	Select the <b>Add NSSAI</b> button to add a NSSAI to your test configuration.
<i>SMF NSSAI:</i>	
	Select the <b>Delete NSSAI</b> 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.

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

<b>Setting</b>	<b>Description</b>
<i>Targeted Nodes</i>	
	Select this button to add the a target node to your test configuration.
<i>Settings</i>	
Target Node	
	Select the <b>Delete Target Node</b> 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.

Setting	Description
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"> <li>• <b>SUBSCRIPTION</b></li> <li>• <b>POLICY</b></li> <li>• <b>EXPOSURE</b></li> <li>• <b>APPLICATION</b></li> </ul>
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 <b>Delete Target Plmn</b> button to remove this list from your test configuration.
PLMN MCC	Provide the PLMN MCC (Mobile Country Code) value.

Setting	Description
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.

## 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	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.

<b>Connectivity Settings</b>	<b>Description</b>
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>	<b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

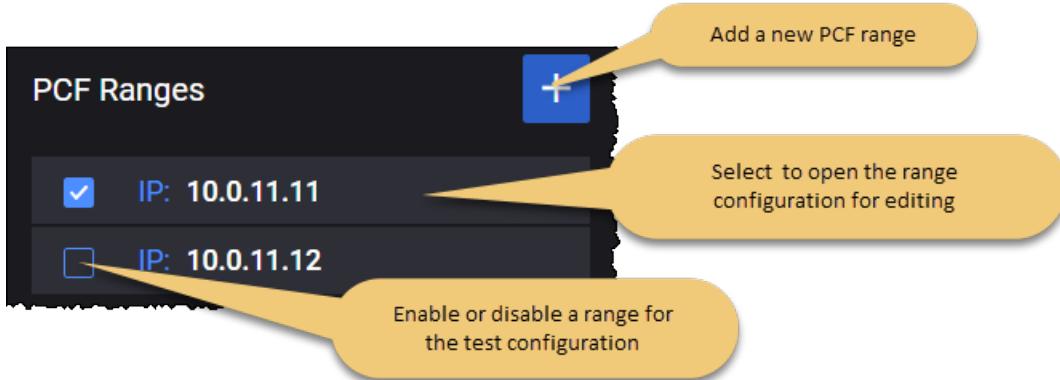
## PCF configuration settings

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.

<b>Setting</b>	<b>Description</b>
<i>PCF:</i>	
	Select the <b>Delete Range</b> 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 <a href="#">PCF Npcf interface settings</a> 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><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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</p>

Setting	Description
	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.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
Indirect Communication without Delegated Discovery	This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a> .
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 <a href="#">SCP Connection Settings</a> .
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 <a href="#">Optional Discovery Parameters</a> .

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 <b>Delete Target Node</b> button to remove this node from your test configuration.
<i>Target Type</i>	Select the target node from the drop-down list.

<b>Setting</b>	<b>Description</b>
<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"> <li>• <b>SUBSCRIPTION</b></li> <li>• <b>POLICY</b></li> <li>• <b>EXPOSURE</b></li> <li>• <b>APPLICATION</b></li> </ul>
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.

Setting	Description
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 <b>Delete Target Plmn</b> 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.

## 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.

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

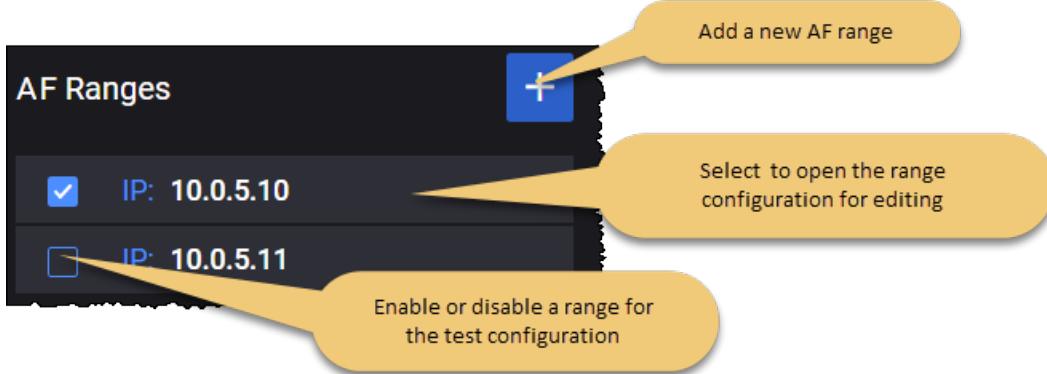
## AF configuration settings

The **AF Ranges** panel opens when you select the AF node from the Simulated Nodes panel.

You can perform the following tasks from this panel:

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

### For example ...



You can add and delete AF ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you need to configure for each AF range.

Setting	Description
<i>AF:</i>	
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
<i>Naf Interface Settings:</i>	
Connectivity Settings	Each AF range requires the configuration of Naf interface settings. These settings are described below in the <a href="#">AF Naf interface settings</a> section.
<i>Node Settings:</i>	
Instance ID	Each AF 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.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
Indirect Communication without Delegated Discovery	This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a> .
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, SMSF) for Indirect Communication via SCP.

Setting	Description
Indirect Communication with Delegated Discovery	This option is available only if SCP is selected in <a href="#">SCP Connection Settings</a> .
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 (UDM, AUSF, PCF, NSSF, SMSF).
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 <a href="#">Optional Discovery Parameters</a> .

## AF Naf interface settings

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

The following **Connectivity Settings** enable the necessary Naf 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).
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.

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

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

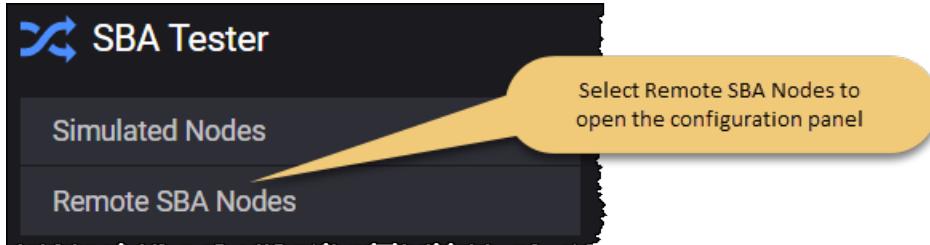
<b>Setting</b>	<b>Description</b>
<i>Target Nodes</i>	
	Select this button to add the a target node to your test configuration.
<i>Settings</i>	
Target Node	
	Select the <b>Delete Target Node</b> button to remove this node from your test configuration.
Target Type	Select the target node from the drop-down 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.

Setting	Description
SUPI	Set the subscription permanent identifier value.
GPSI	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"> <li>• <b>SUBSCRIPTION</b></li> <li>• <b>POLICY</b></li> <li>• <b>EXPOSURE</b></li> <li>• <b>APPLICATION</b></li> </ul>
AMF Region ID	Set the value for this field.
Network Instance Format	Select the encoding format for the network instance: <b>string</b> or <b>label-list</b> .
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 <b>Delete Target Plmn</b> button to remove this list from your test configuration.

<b>Setting</b>	<b>Description</b>
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.

## 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: <b>AUSF, CHF, NSSF, PCF, SMSF and UDM</b>.</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.

<b>Setting</b>	<b>Description</b>
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.

<b>AUSF configuration settings .....</b>	<b>706</b>
AUSF Ranges panel .....	707
AUSF Range panel .....	707
AUSF node settings .....	708
AUSF Nauf interface settings .....	709
AUSF remote SBA nodes .....	710
<b>CHF configuration settings .....</b>	<b>712</b>
CHF Ranges panel .....	712
CHF Range panel .....	713
CHF node settings .....	713
CHF Nchf interface settings .....	714
CHF remote SBA nodes .....	715
<b>NRF configuration settings .....</b>	<b>716</b>
NRF Ranges panel .....	716
NRF Range panel .....	716
NRF node settings .....	717
NRF Nnrf interface settings .....	718
<b>NSSF configuration settings .....</b>	<b>720</b>
NSSF Ranges panel .....	721
NSSF Range panel .....	721
NSSF node settings .....	722
Nnssf Interface Settings .....	723
Remote SBA nodes .....	724
NSSF Restricted NSSAIs .....	725
NSSF Network Slices .....	726
NSSF Configured NSSAI .....	727
<b>PCF configuration settings .....</b>	<b>728</b>
PCF Ranges panel .....	728
PCF Range panel .....	728

PCF node settings .....	729
PCF service area restrictions .....	731
PCF Npcf interface settings .....	732
PCF remote SBA nodes .....	733
<b>SCP configuration settings .....</b>	<b>734</b>
SCP Ranges panel .....	734
SCP Range panel .....	735
SCP Nscp interface settings .....	736
SCP Remote SBA Nodes .....	737
<b>SMSF configuration settings .....</b>	<b>738</b>
SMSF Ranges panel .....	738
SMSF Range panel .....	739
SMSF node settings .....	740
SMSF Nsmsf interface settings .....	740
SMSF Remote SBA Nodes .....	741
<b>UDM configuration settings .....</b>	<b>744</b>
UDM Ranges panel .....	744
UDM Range panel .....	745
UDM node settings .....	746
UDM Nudm interface settings .....	749
UDM remote SBA nodes .....	750
<b>UDR configuration settings .....</b>	<b>751</b>
UDR Ranges panel .....	751
UDR Range panel .....	752
UDR Nudr interface settings .....	754
UDR remote SBA nodes .....	755

## 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:

<b>AUSF Ranges panel</b> .....	<b>707</b>
<b>AUSF Range panel</b> .....	<b>707</b>
<b>AUSF node settings</b> .....	<b>708</b>
<b>AUSF Nausf interface settings</b> .....	<b>709</b>
<b>AUSF remote SBA nodes</b> .....	<b>710</b>

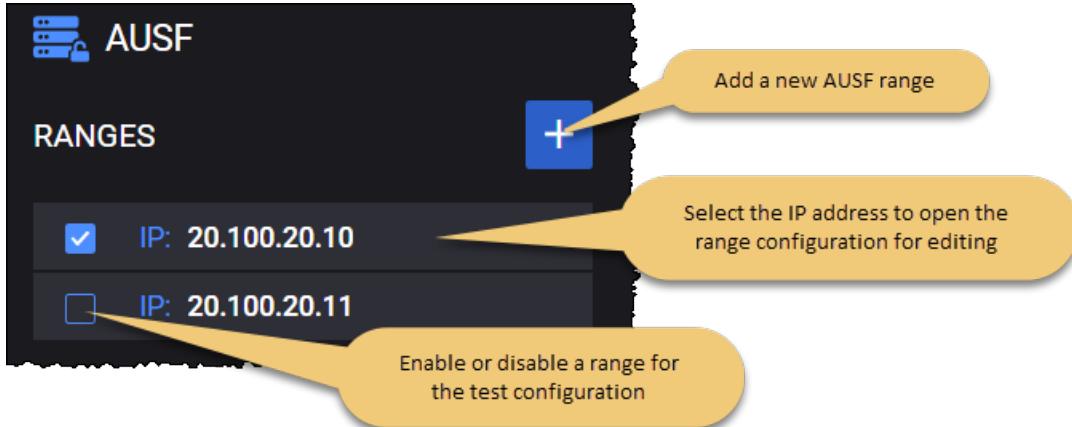
## AUSF Ranges panel

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 <b>Delete Range</b> 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 <a href="#">AUSF node settings</a> .
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 <a href="#">AUSF Nausf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">AUSF remote SBA nodes</a> .

## 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.
PLMN MCC	<p>Set the mobile country code.</p> <p><b>About PLMN MCC ...</b></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>Set the mobile network code.</p> <p><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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 <b>Add Routing Indicator</b> button to add a routing indicator for the AUSF range.
	Select the <b>Delete</b> 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>

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

## 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"> <li>• 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.</li> <li>• Select <b>Discover</b> to invoke the NF discovery service.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> 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.

Setting	Description
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>

## NRF Connection Settings

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

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

## SCP Connection Settings

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

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

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

- **Indirect Communication without Delegated Discovery**

If Indirect Communication 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.

## 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.

<b>CHF Ranges panel</b>	<b>712</b>
<b>CHF Range panel</b>	<b>713</b>
<b>CHF node settings</b>	<b>713</b>
<b>CHF Nchf interface settings</b>	<b>714</b>
<b>CHF remote SBA nodes</b>	<b>715</b>

**Topics:**

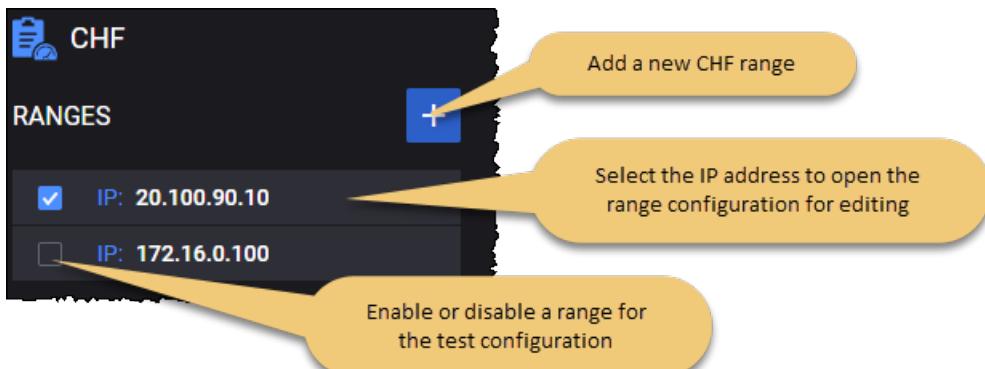
### CHF Ranges panel

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 <b>Delete Range</b> 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 <a href="#">CHF node settings</a> .
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 <a href="#">CHF Nchf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">CHF remote SBA nodes</a> .

### 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.

Setting	Description
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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.
<i>Outer VLAN</i>	<i>Select the check-box to make this option available, and, then, select the Outer</i>

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

## CHF remote SBA nodes

### NRF Connection Settings

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

<b>Setting</b>	<b>Description</b>
<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.

<b>Setting</b>	<b>Description</b>
<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:

<b>NRF Ranges panel</b>	<b>716</b>
<b>NRF Range panel</b>	<b>716</b>
<b>NRF node settings</b>	<b>717</b>
<b>NRF Nnrf interface settings</b>	<b>718</b>

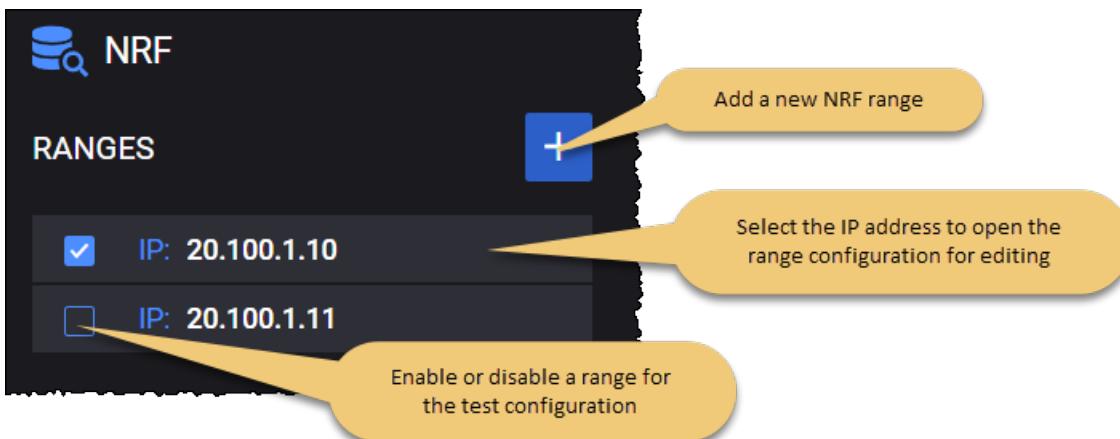
### NRF Ranges panel

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 <b>Delete Range</b> 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 <a href="#">NRF node settings</a> .
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 <a href="#">NRF Nnrf interface settings</a> .

## 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. <b>About PLMN MCC ...</b> 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

Setting	Description
	country of domicile of the mobile subscriber.
MNC	<p>Set the mobile network code.</p> <p><b>About PLMN MNC ...</b></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>
Heartbeat Interval(s)	Time in seconds expected between 2 consecutive heartbeat messages from an NF Instance to the NRF.

## NRF Nnrf interface settings

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

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

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

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

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

## 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:

<b>NSSF Ranges panel</b>	<b>721</b>
<b>NSSF Range panel</b>	<b>721</b>
<b>NSSF node settings</b>	<b>722</b>
<b>Nnssf Interface Settings</b>	<b>723</b>
<b>Remote SBA nodes</b>	<b>724</b>
<b>NSSF Restricted NSSAIs</b>	<b>725</b>
<b>NSSF Network Slices</b>	<b>726</b>
<b>NSSF Configured NSSAI</b>	<b>727</b>

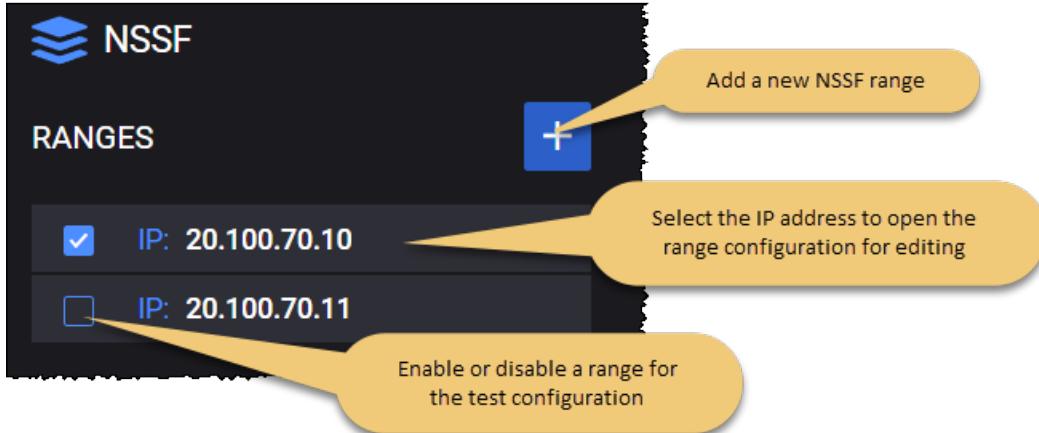
## NSSF Ranges panel

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 <b>Delete Range</b> 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 <a href="#">NSSF node settings</a> .
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 <a href="#">Nnssf Interface Settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">Remote SBA nodes</a> .
<i>Network Slicing:</i>	
Restricted NSSAIs	These settings are described in <a href="#">NSSF Restricted NSSAIs</a> .
Network Slices	These settings are described in <a href="#">NSSF Network Slices</a> .
Configured NSSAIs	These settings are described in <a href="#">NSSF Configured NSSAI</a> .

## NSSF node settings

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

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple NSSF instances may be deployed in the 5G network. Each NSSF instance is uniquely identified by an <i>Instance ID</i> . You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Hostname</i>	
Hostname	The name used to build the fully qualified domain name (FDQN) of this node. If empty, the <b>Instance ID</b> is used as hostname.
PLMN MCC	Set the mobile country code. <b>About PLMN MCC ...</b> 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

Setting	Description
	<p>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>Set the mobile network code.</p> <p><b>About PLMN MNC ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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>

<b>Connectivity Setting</b>	<b>Description</b>
	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>	
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.

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

## SCP Connection Settings

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

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

## NSSF 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 <b>Add a restricted NSSAI</b> button to add a restricted NSSAI to your test configuration.
<i>Restricted NSSAI settings:</i>	
	Select the <b>Delete Restricted NSSAI</b> 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 <b>Add NSSAI</b> button to add a Restricted A-NSSAI to your test configuration.

Setting	Description
<i>NSSAI Settings:</i>	
	Select the <b>Delete NSSAI</b> button to delete this NSSAI from your test configuration.
SST	The default Slice/Service Type (SST) value.
SD	The default Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The default Mapped configure Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The default Mapped configured Slice Differentiator (SD) value for this S-NSSAI.

## NSSF Network Slices

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

Setting	Description
<i>Network Slices:</i>	
	Select the <b>Add a Network slice</b> button to add a network slice to your test configuration.
<i>Network Slice settings:</i>	
	Select the <b>Delete a Network Slice</b> 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>	

Setting	Description
	Select the <b>Add Tracking Area</b> button to add a Tracking Area (TA) to your test configuration.
<i>Tracking Area Indication (TAI) settings:</i>	
	Select the <b>Delete TAI</b> 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 <b>Add a Configured NSSAI</b> button to add a Configured NSSAI to your test configuration.
<i>Configured SNSSAI settings:</i>	
	Select the <b>Delete a Configured NSSAI</b> 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 <b>NSSF Network Slices</b> 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:

<b>PCF Ranges panel</b>	<b>728</b>
<b>PCF Range panel</b>	<b>728</b>
<b>PCF node settings</b>	<b>729</b>
<b>PCF service area restrictions</b>	<b>731</b>
<b>PCF Npcf interface settings</b>	<b>732</b>
<b>PCF remote SBA nodes</b>	<b>733</b>

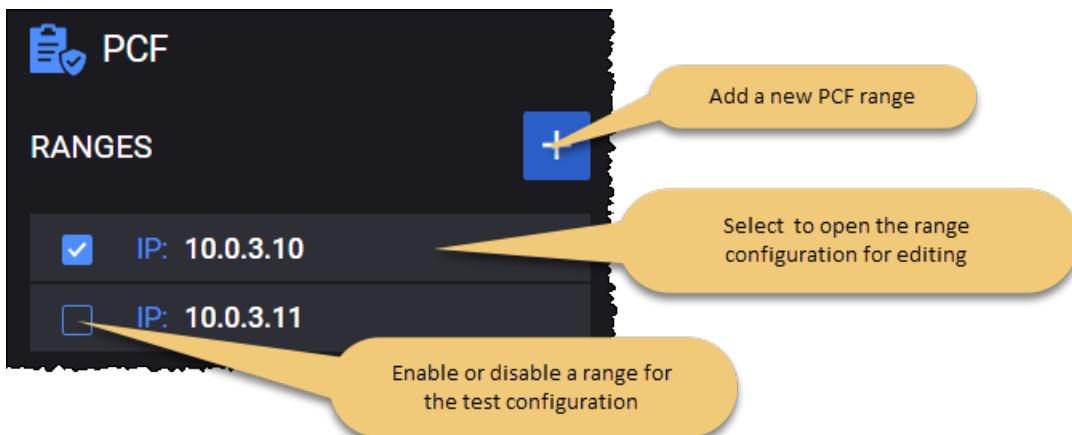
### PCF Ranges panel

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 <b>Delete Range</b> 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 includes the configuration of an associated set of Node Settings, which are described in <a href="#">PCF node settings</a> .
Service Area Restrictions	Each PCF range requires the configuration of the service area restrictions. The settings are described in <a href="#">PCF service area restrictions</a> .
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 <a href="#">PCF Npcf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">PCF remote SBA nodes</a> .

## 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.
Name	The name of the PCF range. You can accept the name provided by the LoadCore, or

<b>Setting</b>	<b>Description</b>
	you can replace it with a name of your own choosing.
PLMN MCC	<p>The PLMN MCC for this PCF range.</p> <p><b>About PLMN MCC ...</b></p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this PCF range.</p> <p><b>About PLMN MNC ...</b></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.
Retrieve Operator Specific Data	Retrieve Operator Specific Data from UDR during SM Policy Establishment.
Retrieve AM Policy Data	If enabled, the PCF will retrieve AM Policy data from UDR.
Triggers	Request Triggers to which the PCF subscribes. The allowed values are:

Setting	Description
	<ul style="list-style-type: none"> <li>• Location Change (tracking area). The tracking area of the UE has changed.</li> <li>• PRA Change (change of UE presence in PRA). The UE is entering/leaving a Presence Reporting Area.</li> <li>• Service Area Restriction Change</li> <li>• RFSP CHRA Change</li> <li>• Manage UE Policy Message</li> </ul> <p>Multiple values can be selected simultaneously.</p>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## PCF service area restrictions

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

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

Setting	Description
<i>Service Area Restrictions:</i>	
Restriction type	Set the restriction type attribute: <ul style="list-style-type: none"> <li>• Allowed Areas</li> <li>• Not Allowed Areas</li> </ul>
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 <b>Add Area</b> button to add a new restriction area to your configuration.
<i>Area:</i>	
	Select the <b>Delete Area</b> button to remove the restriction area from your configuration.
Area Codes	Set the area code. Location Area Code (LAC) is a fixed length code (two octets) identifying a location area within a PLMN.

Setting	Description
TACS:	
	<p>This represents the Tracking Area Code (TAC) for this eNodeB. Select the <b>Add TAC</b> 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 <b>Delete</b> 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
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.

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

## 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.

<b>Setting</b>	<b>Description</b>
<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.

Setting	Description
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.
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:

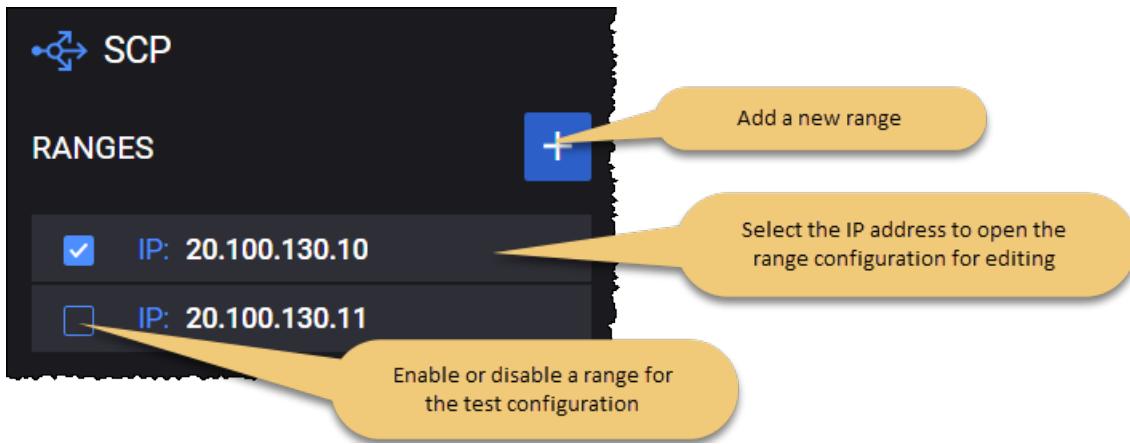
<b>SCP Ranges panel</b> .....	<b>734</b>
<b>SCP Range panel</b> .....	<b>735</b>
<b>SCP Nscp interface settings</b> .....	<b>736</b>
<b>SCP Remote SBA Nodes</b> .....	<b>737</b>

### 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 <b>Delete Range</b> 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 <a href="#">SCP node settings</a> .
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 <a href="#">SCP Nscp interface settings</a> .
Remote SBA Nodes	The remote SBA node settings are described in <a href="#">SCP remote SBA nodes</a> .

## 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 Delegated Discovery	Select this option to enable delegated discovery.
HTTP Connections	The number of HTTP connections between two nodes.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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	The additional routes will use the gateway defined in the IP information below.

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

## SCP Remote SBA Nodes

### Peer SCP Type

<b>Setting</b>	<b>Description</b>
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**.

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

## NRF Connection Settings

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

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

## SMSF configuration settings



Short Message Service Function (SMSF) is the 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:

<b>SMSF Ranges panel</b> .....	<b>738</b>
<b>SMSF Range panel</b> .....	<b>739</b>
<b>SMSF node settings</b> .....	<b>740</b>
<b>SMSF Nsmsf interface settings</b> .....	<b>740</b>
<b>SMSF Remote SBA Nodes</b> .....	<b>741</b>

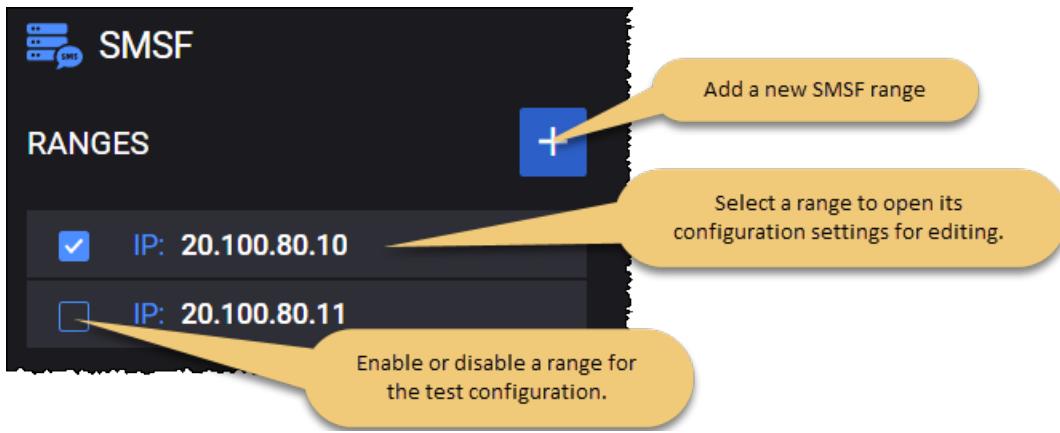
### SMSF Ranges panel

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 <b>Delete Range</b> 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 <a href="#">SMSF node settings</a> .
Nsmsf 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 <a href="#">SMSF Nsmsf interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">SMSF remote SBA nodes</a> .

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.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.

## 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	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>

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

## SMSF Remote SBA Nodes

### AMF Connection Settings

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

<b>Setting</b>	<b>Description</b>
<i>AMF Connectivity Settings:</i>	
Peer AMF type	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> <li>• Select <b>Preset</b> - this option allows manually configuration of a peer AMF, as described <a href="#">here</a>.</li> <li>• Select <b>Discover</b> to invoke the NF discovery service. The SMSF will discover the AMF.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect Communication without Delegated Discovery</a>.</p>

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

The following table describes the settings required to configure a preset peer AMF:

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

## UDM Connection Settings

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

Setting	Description
<i>UDM Connectivity Settings:</i>	
Peer UDM type	<p>Select the peer UDM using either of the following methods:</p> <ul style="list-style-type: none"> <li>Select <b>None</b> - no N21 interface.</li> <li>Select <b>Preset</b> - active N21 interface, this option allows manually configuration of a peer UDM, as described <a href="#">here</a>.</li> <li>Select <b>Discover</b> - active N21 interface, the peer UDM is discovered via NRF.</li> </ul> <p>Refer to <a href="#">NF Discovery service</a> for the steps required to use the discovery service.</p>
Indirect Communication without Delegated Discovery	<p><b>IMPORTANT</b> 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 <a href="#">Indirect</a></p>

Setting	Description
	<a href="#">Communication without Delegated Discovery.</a>
Indirect Communication with Delegated Discovery	<p><b>IMPORTANT</b> This option is visible only when Peer UDM is set to <b>Discover</b> and SCP is selected in SCP Connection Settings.</p> <p>Select the option to enable it. For more details, refer to <a href="#">Indirect Communication with Delegated Discovery</a>.</p>

The following table describes the settings required to configure a preset peer UDM:

Setting	Description
<i>UDM Peers:</i>	
	Select this button to add the peer UDM to your test configuration.
<i>UDM Peer:</i>	
	Select this button to delete the peer UDM from your test configuration.
Peer UDM	Select the peer UDM 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.

## NRF Connection Settings

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

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

## SCP Connection Settings

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

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

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.

## 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:

<b>UDM Ranges panel</b>	<b>744</b>
<b>UDM Range panel</b>	<b>745</b>
<b>UDM node settings</b>	<b>746</b>
<b>UDM Nudm interface settings</b>	<b>749</b>
<b>UDM remote SBA nodes</b>	<b>750</b>

### 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 <b>Delete Range</b> 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	Each UDM range has the configuration of an associated set of Node Settings, which are

Setting	Description
Settings	described in <a href="#">UDM node settings</a> .
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 <a href="#">UDM Nudm interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">UDM remote SBA nodes</a> .

## 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.
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><b>About SUPI and SUCI ...</b></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>
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
PLMN MCC	<p>The PLMN MCC for this UDM range.</p> <p><b>About PLMN MCC ...</b></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</p>

Setting	Description
	<p>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><b>About PLMN MNC ...</b></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 <b>Add Routing Indicator</b> button to add a Routing Indicator for the UDM range.
	Select the <b>Delete</b> 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 <b>Delete Subscription</b> button to remove this subscription from the SDM notifications.
Resource name	This represents the subscribed resource (entered as a string) for which notifications are triggered. Valid strings currently supported: <i>nssai, am-data, smf-select-data, sm-data, ue-context-in-smf-data</i> .
Notification trigger time (ms)	This represents the time interval (in milliseconds) from NF subscription (for that resource) after which that NF will start receiving notifications from UDM.
Change resource continuously	Select this option to apply the changes from the list continuously(start over again when reaching the end of the list). If this option is not selected, the notifications for the resource will stop when the last change in the list will happen, otherwise they will start from the beginning again.
<i>Resource changes:</i>	
	Select the <b>Add change</b> button to add new list of changes that will happen over time to the defined resource.
<i>Change Item</i>	
	Select the <b>Delete Change Item</b> to remove this list from your configuration.
Change type	This represents the nature of the change: <ul style="list-style-type: none"> <li>• <b>Add</b> - new content was added to the resource.</li> <li>• <b>Change</b> - a certain content has changed.</li> <li>• <b>Remove</b> - a certain content was removed.</li> <li>• <b>Move</b> - a certain content has been moved from one place to another.</li> </ul>
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 <a href="#">Path in resource to change</a> . <div style="background-color: #0070C0; color: white; padding: 2px 10px; margin-left: 10px;"><b>IMPORTANT</b></div> This field must have a valid JSON text value only if the <a href="#">Change type</a> is set to <b>Add</b> or <b>Replace</b> .

Setting	Description
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 <a href="#">Notification Trigger timer</a> .
From source path (used for Move change type)	<p><b>NOTE</b> This parameter is available only when <a href="#">Change type</a> is set to <b>Move</b>.</p> <p>This represents the original path of the JSON object that has been moved.</p>

## UDM Nudm interface settings

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

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

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

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

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

## UDM remote SBA nodes

### NRF Connection Settings

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

<b>Setting</b>	<b>Description</b>
<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.

<b>Setting</b>	<b>Description</b>
<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.

## 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:

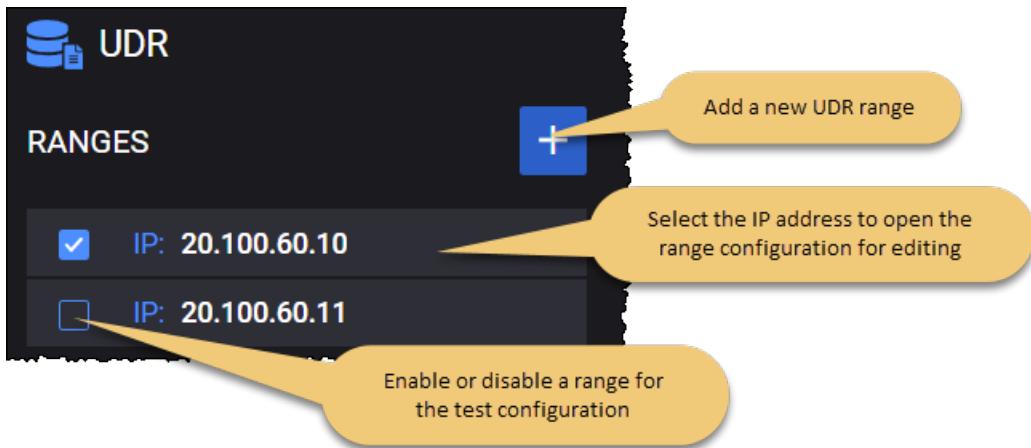
<b>UDR Ranges panel</b> .....	<b>751</b>
<b>UDR Range panel</b> .....	<b>752</b>
<b>UDR Nudr interface settings</b> .....	<b>754</b>
<b>UDR remote SBA nodes</b> .....	<b>755</b>

## 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 ...



If multiple agents are assigned to the UDR node, the **Distribution Mode** parameter is displayed and the following options can be selected from the drop-down:

- **All Ranges on All Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UDR node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1 and agent2, range2 on agent1 and agent2, range 3 on agent1 and agent2.
- **Round Robin Ranges on Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UDR node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1, range2 on agent2, range3 on agent1.

## 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 <b>Delete Range</b> 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).

Setting	Description
<i>Range Settings:</i>	
Node Settings	Each UDR range requires the configuration of an associated set of Node Settings, which are described in <a href="#">UDR node settings</a> .
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 <a href="#">UDR Nudr interface settings</a> .
Remote SBA Nodes	These settings are described in <a href="#">UDR remote SBA nodes</a> .

## Node Settings

The following table describes the available UDR Node Settings.

Setting	Description
Instance ID	<p>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.</p> <p>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.</p>
Name	The name of the UDR range. You can accept the name provided by the LoadCore, or you can replace it with a name of your own choosing.
HTTP2 User Agent	User-Agent header in HTTP2 requests initiated from this node. For more details, see 3GPP TS 29.500, Table 5.2.2.2-1.
PLMN MCC	<p>Set the mobile country code.</p> <p><b>About PLMN MCC ...</b></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>Set the mobile network code.</p> <p><b>About PLMN MNC ...</b></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>

## 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner</i></p>

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

## UDR remote SBA nodes

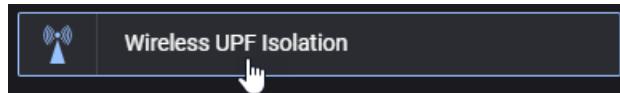
To connect to the Network Repository Function (NRF) node, the following configuration settings are required.

<b>Setting</b>	<b>Description</b>
<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 9*

## **UPF Isolation tests: configuration settings**

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



In an UPF Isolation test topology, the DUT is UPF and LoadCore simulates traffic on the N3, N4, and N6 interfaces. You configure the simulated UEs, NG-RAN, SMF, and DN as required by your test requirements.

**Topics:**

<b>Global Settings panel</b> .....	<b>758</b>
DNS Settings .....	759
Advanced Settings .....	759
Impairment .....	762
QoS Flows panel .....	763
QoS Flow configuration settings .....	763
Reporting Settings .....	765
External Stats Server .....	765
Global Playlists .....	772
<b>UE configuration settings</b> .....	<b>774</b>
UE Ranges panel .....	775
UE Range panel .....	776
UE range settings .....	777
Objectives .....	783
Control Plane Objective .....	783
User Plane Objectives .....	796
<b>RAN configuration settings</b> .....	<b>851</b>
RAN Ranges panel .....	852

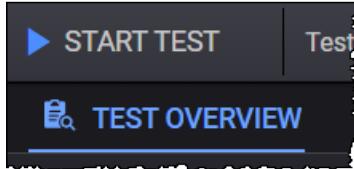
RAN Range settings .....	852
RAN N3 interface settings .....	853
Passthrough interface settings .....	854
<b>SMF configuration settings .....</b>	<b>855</b>
SMF Ranges panel .....	856
SMF Range settings .....	856
SMF N4 interface settings .....	857
SMF Uplink Paths .....	859
<b>UPF configuration settings .....</b>	<b>861</b>
UPF Ranges panel .....	862
UPF Range panel .....	862
UPF N3 interface settings .....	863
UPF N4 interface settings .....	865
UPF N6 interface settings .....	866
UPF N9 interface settings .....	867
UPF N4u interface settings .....	869
<b>DN configuration settings .....</b>	<b>872</b>
DN Ranges panel .....	872
DN Range panel .....	873
DN N6 Interface settings .....	874
DN routes settings .....	875
DN User Plane .....	876
DN Stateless UDP Traffic .....	877
DN Data Traffic .....	878
DN Voice Traffic .....	881
DN Video OTT Traffic .....	894
DN DNS Server Traffic .....	897
DN Predefined Applications Traffic .....	899
DN Capture Replay .....	899
DN Synthetic .....	901
DN UDG .....	903
DN Throttling settings .....	905

## 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:

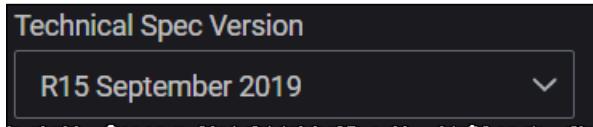


2. Click **Expand** if the Test Overview section is collapsed.
3. Click the Global Settings' **Edit** button:



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:

<b>DNS Settings</b>	759
<b>Advanced Settings</b>	759
<b>Impairment</b>	762
<b>QoS Flows panel</b>	763
QoS Flow configuration settings	763
Reporting Settings	765
<b>External Stats Server</b>	765
<b>Global Playlists</b>	772

## DNS Settings

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

The DNS information is used only for the user plane path, that is, the configured DNS Server is used to resolve the destination configured for the user plane objectives in case the destination is a host name and not an IP.

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 <b>Add DNS Name Server</b> button to add a new DNS server to your test configuration. Set the IP address of the DNS server.
	Select the <b>Delete</b> 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	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size	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.
Power Saver on Agents	Select this option to disable the IxStack/DPDK at the end of each test on all agents.
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"> <li>• <b>None</b> - no advanced statistics enabled.</li> <li>• <b>One Way Delay</b> - the time spent by the packet on the network from the moment it is sent until it is received.</li> <li>• <b>Delay Variation Jitter</b> - the per polling interval average delay variation jitter value calculated for all packets.</li> </ul>
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"> <li>• <b>Info</b> - Designates informational messages that highlight the progress of the application at coarse-grained level.</li> <li>• <b>Debug</b> - Designates fine-grained informational events that are most useful to debug the application.</li> </ul>
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.
Traffic Settings	See <a href="#">Traffic Settings</a>
Response Cache	See <a href="#">Response Cache Settings</a> .

## Traffic Settings

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

Setting	Description
GTPU Source Port:	

<b>Setting</b>	<b>Description</b>
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.
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	
Traffic Control Port	Set the traffic control port. By default, it is set to 44556.
Enable Jumbo Frame	Enable this option if your test traffic requires the use of jumbo frames (Ethernet frames with more than 1500 bytes of payload). When you enable this option, you can then configure any of the MTU parameters in the test to any valid jumbo frame size (up to 9,000 bytes).
Enable IxStack L4 Port Randomization	Select this option to enable IxStack L4 Port Randomization.
Enable UDP Port Recycling	Select this option to enable IxStack UDP Port Recycling.
Enable TCP Port Recycling	Select this option to enable IxStack TCP Port Recycling.
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).

## Response Cache Settings

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

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

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

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

## Impairment

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

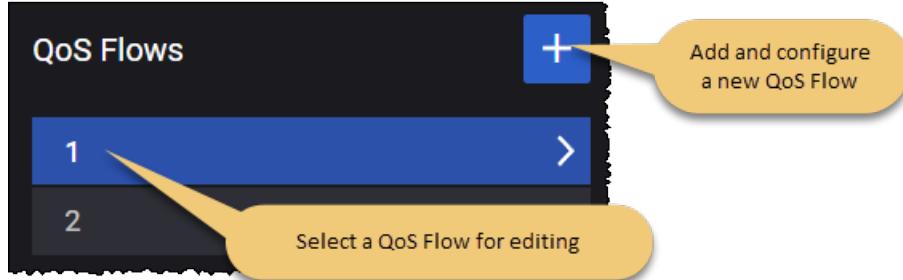
Setting	Description
<i>Impairment Profiles:</i>	
	Select the <b>Add impairment profile</b> button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete impairment profile</b> button to remove the profile from your test configuration.
Name	Each impairment profile 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"> <li>• Custom script</li> <li>• PFCP-drop message</li> </ul>
Script file	This parameter is available only when <b>Action Type</b> is set to <b>Custom script</b> . It allows you to add a custom script, using the <b>Upload</b> button. To remove the script, select the <b>Clear</b> 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** ..... **763**

**Reporting Settings** ..... **765**

### 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 <b>SDF</b> 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"> <li>• the Action is 'permit'</li> <li>• the Direction is 'out'</li> <li>• the Protocol Number is 17 (UDP)</li> <li>• the Source IP address is 22.22.22.22</li> <li>• the Source Port is 11111</li> <li>• The Destination IP is \$ueip\$ (a format specifier for UE IP address)</li> <li>• The Destination Port is 11100.</li> </ul> <p>The SDF String option is available for any QoS flow, including the default flow (s).</p> <p>The SDF syntax details are described in TS 29.212, section 5.4.2.</p>
<i>MBR</i>	
Uplink (kbps)	The MBR uplink bitrate.
Downlink (kbps)	The MBR downlink bitrate.
<i>GBR</i>	
Uplink (kbps)	The GBR uplink bitrate.
Downlink (kbps)	The GBR downlink bitrate.

## Activate predefined rules

This option is used to add a predefined rule on a per flow basis.

**NOTE**

For backwards compatibility, rules can still be activated on a per UE Range basis ([Activate Predefined Rules](#)). If rules are configured on both UE range and QoS Flow, the QoS Flow settings will take precedence.

The **Active Predefined Rules** settings are described in the following table.

<i>Active Predefined Rules:</i>	
	Select the <b>Add Activate Predefined Rules</b> button to add a predefined rule to your test configuration.
	Select the <b>Delete</b> 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.

<b>Setting</b>	<b>Description</b>
<i>Volume Threshold</i>	
Total	The number of octets for the <b>Total Volume</b> field of the Volume Threshold IE.
Uplink	The number of octets for the <b>Uplink Volume</b> field of the Volume Threshold IE.
Downlink	The number of octets for the <b>Downlink Volume</b> field of the Volume Threshold IE.
<i>Volume Quota</i>	
Total	The number of octets for the <b>Total Volume</b> field of the Volume Quota IE.
Uplink	The number of octets for the <b>Uplink Volume</b> field of the Volume Quota IE.
Downlink	The number of octets for the <b>Downlink Volume</b> field of the Volume Quota IE.

## External Stats Server

If this option is selected, it will allow you to add an external statistic server.

The following table describes the settings required for the External Stats Server configuration.

<b>Setting</b>	<b>Description</b>
<i>External Stats Server:</i>	
Profile	This parameter allows you to upload or remove a stats server profile. Press <b>Upload</b>

Setting	Description
	and load the preferred server profile, or <b>Clear</b> to dismiss one that is set.
Server Address	The address of the external stats server.

## Setting up a Profile

The External Stats Server feature allows you to forward statistic logs to an external server, thus requiring to upload a profile that defines where the stats are stored and what stats should be transferred.

**IMPORTANT** This feature is designed to support any type of external entity, but currently it supports only the Apache Kafka Plugin.

The parameters required to create the request to the external entity are configured in the **Profile** JSON file that is uploaded to Keysight Open RAN Simulators, Cloud Edition 5.1. The following structure and parameters describe the standard content of the JSON file:

Section/ Parameter	Definition	Code Sample
<i>Input section</i>	<i>Lists all the stats/config parameters used in the profile. All the parameters are already available in Keysight Open RAN Simulators, Cloud Edition 5.1. the following types are supported:</i>	
stat	It can be any stat supported in Keysight Open RAN Simulators, Cloud Edition 5.1. The stats can be filtered by any other stat from the stat response.	<p>With filter sample:</p> <pre>{   "type": "stat",   "group": "AgentStatistics",   "stat": "CPU Percent",   "name": "cpu_percent1",   "filterBy": {     "stat": "agentIP",     "value": "10.38.158.83"   } }</pre> <p>Without filter sample:</p> <pre>{   "type": "stat",   "group": "Fullcoreoverview_RegisteredAttachedUE",   "stat": "UEs Registered",   "name": "no_of_UE_Registered" }</pre>

Section/ Parameter	Definition	Code Sample
config	It can be any parameter exposed in the UI. The path is the same as the one used by the UI to set/get a parameter (see <a href="#">Parameter sample path below</a> image).	<pre>{   "type": "config",   "group": "config/nodes/ausf/ranges/1/nodeSettings",   "stat": "mcc",   "name": "mcc" }</pre>
<i>Mappings section</i>	<i>Mapping will use any input parameter referred by name. Mapping also supports mathematical expressions to combine stats.</i>	
	<p>For example, Keysight Open RAN Simulators, Cloud Edition 5.1 exposes <code>stat1</code> and <code>stat2</code> but the user needs <code>user_stat</code> which comprises <math>(\text{stat1} + \text{stat2}) / 100</math>. The expression is evaluated and the result sent under <code>user_stat</code> name.</p>	<ul style="list-style-type: none"> <li>one parameter sample:</li> </ul> <pre>{   "type": "controlplane",   "from": "no_of_UE_Registered",   "to": "no_of_UE_Registered" }</pre> <p>OR</p> <pre>{   "type": "controlplane",   "from": "mcc",   "to": "MCC" }</pre> <ul style="list-style-type: none"> <li>with mathematical expression:</li> </ul> <pre>{   "type": "controlplane",   "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",   "to": "agent1 cpu ratio" }</pre>

### Parameter sample path

```
{
  "instanceId": "7ea3abc7-f0f6-435b-9154-125deddd101b",
  "mcc": "226",
  "mnc": "04",
  "routingIndicators": [
    1234,
    2222
  ],
  "links": [
    {
      "rel": "self",
      "type": "self",
      "method": "GET",
      "href": "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings"
    },
    {
      "rel": "meta",
      "type": "meta",
      "method": "GET",
      "href": "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings/$options"
    }
  ]
}
```

## Sample profile

```
{
  "profile": {
    "type": "kafka",
    "3gpp_scenario": "QUIC_ABR_DEBUG",
    "event_type": "ATTS_TOOLS_KEYSIGHT_EVENT",
    "specversion": "1.1",
    "kafkatopics": "com.att.ant.stage.ATTSSKeysight.1.0",
    "kafkaschemaUrl": "https%3A%2F%2Fc1001.eastus2.uat.iebus.3pc.att.com%3A8082%2Fschemas%2Fids%2F6635&schemaId=14260",
    "kafkaHeaderBootstrapUrl": "c1001.eastus2.uat.iebus.3pc.att.com:9093",
    "kafkaHeaderSaslMechanism": "PLAIN",
    "kafkaHeaderOAuthScope": "ANT-data-feed-dev-stage",
    "kafkaUsername": "m30317@ant.att.com",
    "kafkaPassword": "August2023#",
    "input": [
      {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent1",
        "filterBy": {
          "stat": "agentIP",
          "value": "10.38.158.83"
        }
      },
      {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent2",
        "filterBy": {
          "stat": "agentIP",
          "value": "10.38.158.83"
        }
      }
    ]
  }
}
```

```

        "value": "10.38.157.97"
    }
},
{
    "type": "config",
    "group": "config/nodes/ausf/ranges/1/nodeSettings",
    "stat": "mcc",
    "name": "mcc"
},
{
    "type": "config",
    "group":
"config/nodes/ue/ranges/1/userPlane/tigerObjective/1/statelessUDP",
    "stat": "ipAddress",
    "name": "ipAddress"
},
{
    "type": "stat",
    "group": "Fullcoreoverview_RegisteredAttachedUE",
    "stat": "UEs Registered",
    "name": "no_of_UE_Registered"
},
{
    "type": "stat",
    "group": "Fullcoreoverview_PDUSessionEstablishment",
    "stat": "PDU Session Establishment Succeeded",
    "name": "no_of_PDU_Session_Established"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
    "stat": "L2-3 Device Rx Traffic",
    "name": "L3 Server::Total Bits/Sec"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
    "stat": "L2-3 Device Tx Traffic",
    "name": "L3 Client::Total Bits/Sec"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_TCPConnections",
    "stat": "TCP connections established",
    "name": "HTTP/s Handshakes Succeeded"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_TCPConnections",
    "stat": "TCP connect failed",
    "name": "HTTP/s Handshakes Failed"
}

```

```

},
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_TCPConnections",
  "stat": "TCP connections closed normally",
  "name": "HTTP/s Connection Closed"
}
],
"mappings": [
  {
    "type": "controlplane",
    "from": "cpu_percent1 + cpu_percent2",
    "to": "total cpu_percent %"
  },
  {
    "type": "controlplane",
    "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",
    "to": "agent1 cpu ratio"
  },
  {
    "type": "controlplane",
    "from": "cpu_percent2/(cpu_percent1 + cpu_percent2)",
    "to": "agent2 cpu ratio"
  },
  {
    "type": "controlplane",
    "from": "mcc",
    "to": "MCC"
  },
  {
    "type": "controlplane",
    "from": "ipAddress",
    "to": "Destination IP Address"
  },
  {
    "type": "controlplane",
    "from": "no_of_UE_Registered",
    "to": "no_of_UE_Registered"
  },
  {
    "type": "controlplane",
    "from": "no_of_PDU_Session_Established",
    "to": "no_of_PDU_Session_Established"
  },
  {
    "type": "userplane",
    "from": "L3 Server::Total Bits/Sec",
    "to": "L3 Server::Total Bits/Sec"
  },
  {
    "type": "userplane",
    "from": "L3 Server::Total Bits/Sec"
  }
]

```

```

        "from": "L3 Client::Total Bits/Sec",
        "to": "L3 Client::Total Bits/Sec"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Handshakes Succeeded",
        "to": "HTTP/s Handshakes Succeeded"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Handshakes Failed",
        "to": "HTTP/s Handshakes Failed"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Connection Closed",
        "to": "HTTP/s Connection Closed"
    }
]
}
}

```

**Event body sent to Kafka**

```

[
{
    "eventBody": {
        "id": "wireless-0acbc45b-8777-4250-a3ec-4f00e47399c8_39",
        "time": "2024-02-29T13:57:35Z",
        "type": "ATTS-TOOLS-KEYSIGHT-EVENT",
        "specversion": "1.1",
        "source": "https://10.38.157.61/wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
        "datacontenttype": "application/json",
        "payload": [
            {
                "type": "resource_info",
                "resource_info": {
                    "simulated_tool_info": [
                        {
                            "tool_name": "LoadCore",
                            "middleware_ip": "10.38.157.61"
                        }
                    ],
                    "network_type": "5G",
                    "3gpp_scenario": "QUIC_ABR_DEBUG"
                }
            },
            {
                "type": "test_execution_result",
            }
        ]
    }
}
]

```

```

    "test_execution_result": {
        "control_plane_result": {
            "Destination IP Address": "20.0.6.10",
            "MCC": "226",
            "agent1 cpu ratio": "0.455321",
            "agent2 cpu ratio": "0.544679",
            "no_of_PDU_Session_Established": "100",
            "no_of_UE_Registered": "0",
            "total cpu_percent %": "3.0902"
        },
        "userplane_plane_result": {
            "L3 Client::Total Bits/Sec": "0",
            "L3 Server::Total Bits/Sec": "0"
        }
    },
    {
        "type": "test_execution_details",
        "test_execution_details": {
            "testName": "4 - Full Core Base Config",
            "testSessionID": "wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
            "UserID": "admin@example.org",
            "testStatus": "STOPPING",
            "testStartTime": "2024-02-29T13:55:40Z",
            "testDuration": 105,
            "testStopTime": "2024-02-29T13:57:31Z"
        }
    }
],
},
"payloadType": "JSON",
"value": {}
}
]

```

## Global Playlists

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

Setting	Description
<i>Global Playlists:</i>	
	Select the <b>Add Global Playlist</b> button to add a new playlist to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete Global Playlist</b> button to remove the playlist from your test configuration.

Setting	Description
Name	Each playlist profile is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Playlist file (.csv)	It allows you to add a custom playlist, using the <b>Upload</b> button. To remove the file, select the <b>Clear</b> 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:

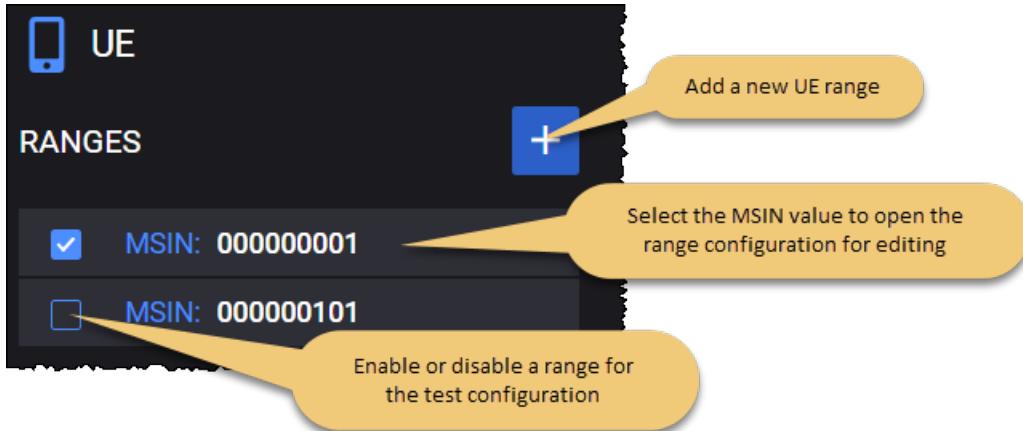
<b>UE Ranges panel</b> .....	<b>775</b>
<b>UE Range panel</b> .....	<b>776</b>
UE range settings .....	777
<b>Objectives</b> .....	<b>783</b>
Control Plane Objective .....	783
User Plane Objectives .....	796

## 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.

If multiple agents are assigned to the UE, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **All UE Ranges and RAN Ranges on All Agents** - for example, for a test with 2 agents and 2 UE ranges and 2 RAN ranges, UE range1 and UE range2 and their parent ranges as well as all RAN ranges part of Mobility Path, and Secondary RAN ranges will be distributed to both agent1 and agent2.
- **Round Robin UE Ranges and RAN Ranges per Agent** - for example, if UE range1 is distributed to agent1, parent RAN range as well as all RAN ranges part of the Mobility Path (visited gNB/eNB ranges) and the Secondary RAN ranges will also be distributed on agent1.

## 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 <b>Delete Range</b> 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 <b>Identification</b> settings: <a href="#">Identification settings</a> .
Settings	Refer to the following topic for descriptions of the UE <b>Settings</b> settings: <a href="#">Settings</a> .
QoS Config	Refer to the following topic for descriptions of the UE <b>QoS Config</b> settings: <a href="#">QoS Config settings</a> .

### 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"> <li>IP</li> <li>Ethernet</li> </ul>
IP Type	Select the type of IP address used in test: <ul style="list-style-type: none"> <li>IPv4</li> <li>IPv6</li> <li>IPv4V6</li> </ul>
<i>Ipv4</i>	<i>This option is available only when IP Type is set to <b>IPv4</b>.</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 <b>IPv6</b>.</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 <b>IPv4V6</b>. 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.

<b>Setting</b>	<b>Description</b>
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><b>NOTE</b> 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>
Use PDI Optimization	Enable this option if the user node also supports this feature and performs the F-TEID allocation.
Include SFD when Application Identifier is Configured	If enabled, it will include SFD in PDIs in PFCP messages sent by the SMF even when the Application identifier is configured for QoS Flow.
Network Instance Format	Select the encoding format for the network instance: string or label-list.
Include N3 Network Instance	<p>Default value: <b>True</b> (the option is enabled).</p> <p>When this option is enabled, the SMF will include in PFCP Session Establishment Request the N3 Network instance.</p> <p>The N3 Network instance in PFCP Session Establishment Request will be the N3 Network Instance in UE range settings, or the N3 Network Instance from UPF node in case the N3 Network Instance in UE range settings is empty.</p> <p>When this option is disabled, the SMF will not include the N3 Network instance</p>

<b>Setting</b>	<b>Description</b>
	in the PFCP Session Establishment Request.
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: myHome.com. An empty value is accepted as input for this parameter. When a value is added it will be sent in PFCP Session Establishment Request message in APN IE. This value is the same for all UEs in range. The DNN field supports dynamic values. These values can be obtained with a sequence generator. The sequence can be added anywhere in the DNN name (beginning, middle or end). The syntax is [start_value-end_value,increment].</p> <p><b>NOTE</b> 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"> <li>dnn[4-9, ] an implicit increment of 1 is used</li> <li>dnn[4-9] as above</li> <li>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</li> <li>dnn[4-, ] as above</li> <li>dnn[4-] as above</li> <li>dnn[4] as above</li> </ul> <p>UEs will use the DNN values from the pool in a round robin manner.</p> <p><b>IMPORTANT</b> 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>

Setting	Description
<i>BAR Settings: These settings are used in the Update BAR procedure for idle UEs.</i>	
Delay Before Update BAR	The delay in milliseconds before the UE will send a Session Modification Request with an UpdateBAR IE. This can occur while the UE is in idle (it happens only one time).
Downlink Data Notification Delay	The delay that the UP will apply between receiving a downlink data packet and notifying the CP function about it. Delay Value in integer multiples of 50 milliseconds, or 0 (TS 29244 8.2.28).
Suggested Buffering Packets Count	The count of suggested buffering packets.
User Plane Inactivity	
User Plane Inactivity Timer (s)	This timer contains the inactivity time period, in seconds, to be monitored by the User Plane function. A 0 value (default) indicates that User Plane Inactivity detection and reporting is stopped/not requested. When the value is greater, this feature will also enable the following parameters.
Delay Between PFCP Session Establishment and Suspend Traffic (s)	The time to wait before the UE suspends the traffic (in seconds).
Suspend Traffic Interval (s)	The time, in seconds, in which the traffic from remote side is suspended.
Remote IPv4 (IPv6)	Press the <b>+</b> button to add a remote IPv4 entry, then add the IP Address(es) of the DN.
Paging Throttling	<b>IMPORTANT</b> <i>This option appears only if UPF node's ranges are not set as Device Under Test.</i>
Throttling Criterion	Select the criterion on which two consecutive Paging messages triggered by the downlink traffic should be sent: <ul style="list-style-type: none"> <li>• <b>Seconds</b></li> <li>• <b>Packets</b></li> </ul>
Value	Assign a number of seconds to wait, or packets to skip until Paging is sent again. A value of 0 disables this option.
<i>Active Predefined Rules:</i>	

Setting	Description
	Select the <b>Add Activate Predefined Rules</b> button to add a predefined rule to your test configuration.
	Select the <b>Delete</b> 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.

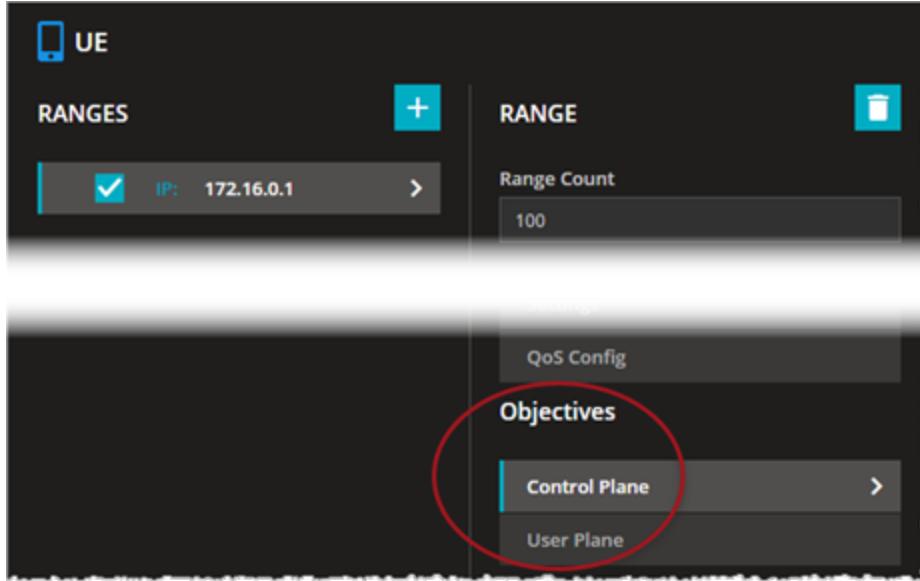
## Objectives

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

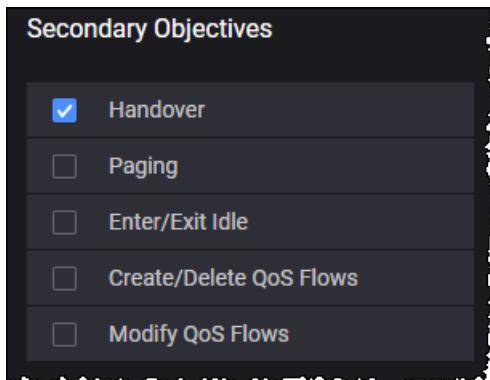
The following table describes the **Primary** control plane objectives.

Parameter	Description
Objective Type	<p>Select the desired Primary Objective Type:</p> <ul style="list-style-type: none"> <li>• <b>Active Subscribers:</b> 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.</li> <li>• <b>Subscribers Per Second:</b> The test attempts to activate a specified number of subscriber sessions per second, within the rate and time parameters that you configure.</li> </ul> <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 (s)	The number of seconds that each subscriber session will remain active. This is, therefore, the amount of time that will elapse between the subscriber attach and the subscriber detach. At the end of the session hold time, the subscriber performs the detach procedure.
Rate	The number of subscriber sessions to activate per second.
Sustain Time (s)	The duration of time (in Seconds) that the specified session activation rate will be maintained.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.

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"> <li>• If the UPF is the DUT in the test topology, then set the <i>Remote IP Address</i> to</li> </ul>

Parameter	Description
	<p>the DN IP address.</p> <ul style="list-style-type: none"> <li>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.</li> </ul>

## 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.

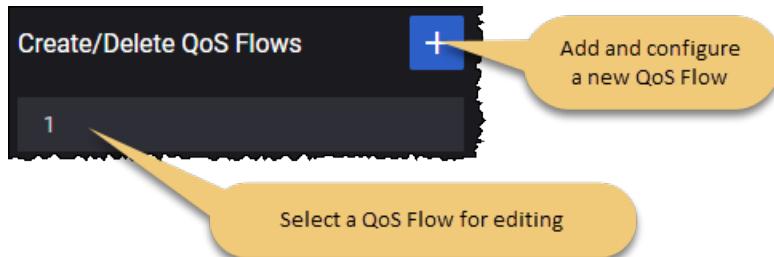
The following table describes the objective parameters.

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 <b>Delete Objective</b> 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.

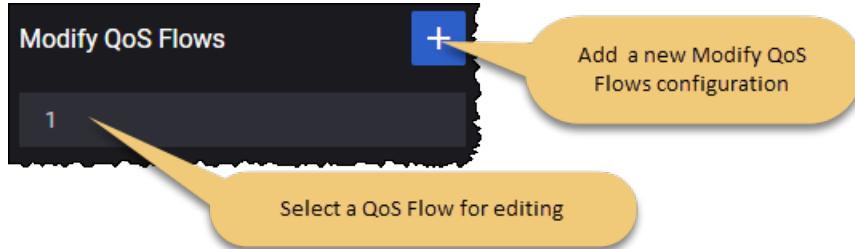
## Modify QoS Flows

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 <b>Delete Objective</b> 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 <a href="#">Update PDR</a> below.
Update QoS	These settings are described in <a href="#">Update QoS</a> below.

Parameter	Description
Update URR	These settings are described in <a href="#">Update URR</a> 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 <b>Delete Update PDR</b> 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 <b>Add Activate Predefined Rules</b> button to add a predefined rule to your test configuration.
	Select the <b>Delete</b> button to remove the redefined rule from your test configuration.
<i>Deactivate Predefined Rules: List of predefined rules to be deactivated.</i>	
	Select the <b>Add Activate Predefined Rules</b> button to deactivate a predefined rule to your test configuration.
	Select the <b>Delete</b> 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.



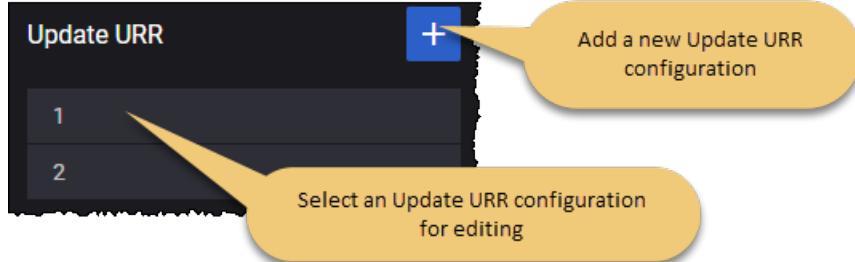
The following table describes the Update QoS settings.

Parameter	Description																				
<i>Update QoS Settings:</i>																					
	Select the <b>Delete Update QoS</b> 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.



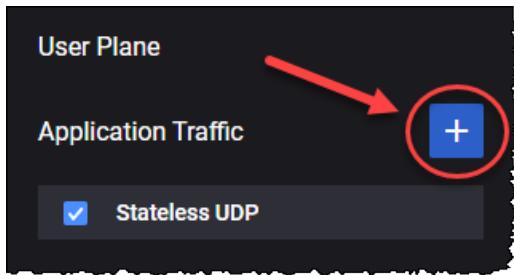
The following table describes the Update URR settings.

Parameter	Description
<i>Update URR Settings:</i>	
	Select the <b>Delete Update URR</b> 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 <b>Total Volume</b> field.
Uplink	Set the value for the <b>Uplink Volume</b> field.
Downlink	Set the value for the <b>Downlink Volume</b> field.
<i>Volume Quota:</i>	
Total	Set the value for the <b>Total Volume</b> field.
Uplink	Set the value for the <b>Uplink Volume</b> field.
Downlink	Set the value for the <b>Downlink Volume</b> 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, Ping, Synthetic and UDG**.

**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"> <li><b>Stateless UDP</b></li> <li><b>Data</b></li> <li><b>Voice</b></li> <li><b>Video OTT</b></li> <li><b>DNS Client</b></li> <li><b>Predefined Applications</b></li> <li><b>Synthetic</b></li> <li><b>UDG</b></li> </ul>
	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 <a href="#">Stateless UDP Traffic</a> .
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">Data</a>

Parameter	Description
	<a href="#">Traffic.</a>
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">Voice Traffic</a> .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">Video OTT Traffic</a> .
DNS Client	For the settings required to configure the DNS Client objective, refer to <a href="#">DNS Client Traffic</a> .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to <a href="#">Predefined Applications Traffic</a> .
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to <a href="#">Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG traffic objective, refer to <a href="#">UDG Traffic</a> .
REST API Client	For the settings required to configure the REST API Client objective, refer to <a href="#">REST API Client</a> .

## 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 <b>Stateless UDP</b> .
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 <b>uplink</b> 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"> <li>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</li> </ul>

Parameter	Description
	<p>back to the default flow.</p> <ul style="list-style-type: none"> <li>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).</li> </ul> <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 <b>Data</b> .
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 <b>Throughput</b> . The other options are: <b>Concurrent Connections</b> and <b>Connections Rate</b> .
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connections Rate per Second	Set the value for connections rate per second. This parameter is available only when Objective type is set to <b>Connections Rate</b> .
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: <b>IPv4</b> or <b>IPv6</b> .
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"> <li>To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul> <p>Refer to <a href="#">Flow</a> for a description of the configuration settings for these traffic flows. Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Flow</b> 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"> <li>If <a href="#">Optimize Throughput (per UE)</a> option is enabled: <b>TCP</b>, <b>TLS</b>, <b>QUIC</b> or <b>UDP</b>.</li> <li>If <a href="#">Optimize Throughput (per UE)</a> option is disabled: <b>TCP</b>, <b>TLS</b> or <b>UDP</b>.</li> </ul>
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get</b>, <b>HTTP Put</b>, <b>HTTP Post</b> and <b>FTP</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get</b>, <b>HTTPS Put</b> and <b>HTTPS Post</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Get</b>, <b>HTTP3 Put</b> and <b>HTTP3 Post</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional</b> (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)</li> </ul> <p><b>NOTE</b> 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.  Iterations number is set for each UE in the range, for example: if there is a range of 1000 UEs , and it has an objective of HTTP GET with 100 iterations, each of those UEs will get 100 HTTP pages.
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server. <p><b>NOTE</b> Setting the page size on UE side will only influence PUT objectives, like HTTP PUT, HTTPS PUT and FTP PUT. To set the page size for GET objectives, the change must be operated on DN side.</p>

Parameter	Description
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
URL	The URL that is being accessed by the flow's protocol.
Destination Hostname	Destination hostname of the server. If DNS hostname resolution is enabled for the flow and Name Servers are configured under Global Settings, this name will be resolved before being used as L7 destination IP for the flow and included in HTTP headers. If empty, the "Address" from the previous fly-out level will be used as L7 destination IP for the flow.
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

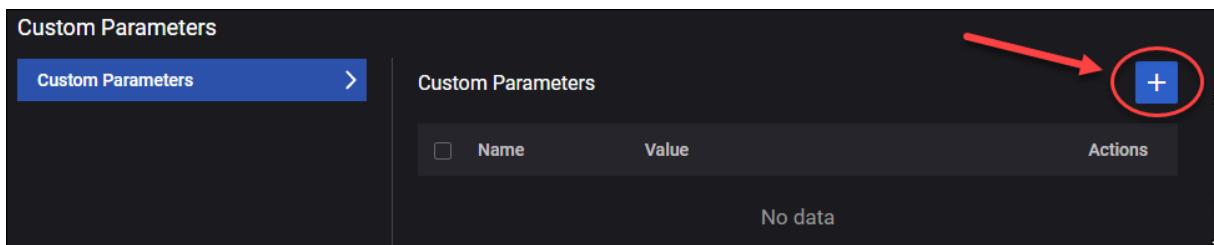
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

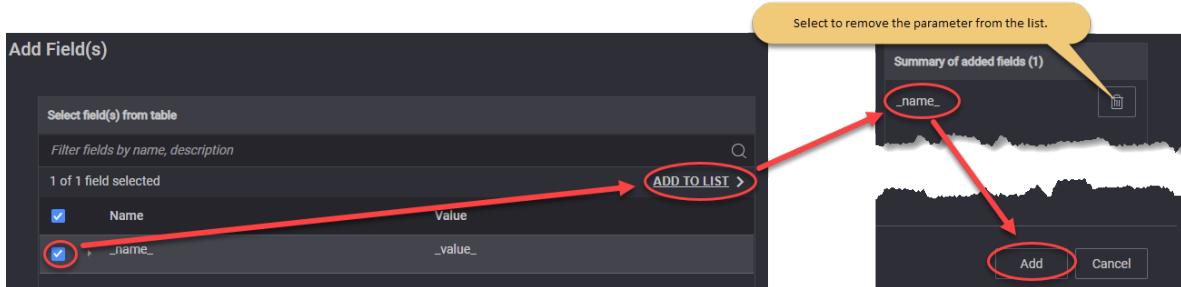
2. Select the **Add** button.



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 <b>Voice</b> .
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 <b>Simulated Users</b> 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.
Call Type	<p>Select the type of call from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>Basic Call</b></li> <li>• <b>Basic Call Mo</b> (Mobile Originated)</li> <li>• <b>Basic Call Mt</b> (Mobile Terminated)</li> <li>• <b>Custom Flow</b></li> </ul> <p>When creating a new test or when adding a new UE range, the Call Type default option is the <b>Basic Call</b>, which allows you to run a basic SIP call without the IMS entity and with DN simulating the Mobile Terminating (MT) side.</p> <p>When selecting <b>Basic Call MO/Basic Call MT</b>, the app will use a predefined SIP Flow intended for the use-case in which a DUT IMS or simulated IMS is involved.</p> <p>If the test requirements need an extended set of SIP flows or higher level of flexibility, it is recommended to use the <b>Custom Flow</b> Call Type, which enables the Flow Editor.</p>
Flow Editor:	<p><b>IMPORTANT</b> This configurator becomes available only if Call Type is set to Custom Flow.</p> <p><i>Click to open the page and create a particular state machine for SIP calls that allows you a higher flexibility to customize the SIP message sequence and SIP</i></p>

Parameter	Description
	<i>headers/SDP body as desired. For settings, refer to <a href="#">Flow Editor</a> section.</i>
Dial Plan:	<i>For the settings required to configure the dial plan, refer to <a href="#">Dial Plan</a>.</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"> <li>• <b>TCP</b> - Transmission Control Protocol</li> <li>• <b>TLS</b> - Transport Layer Security</li> <li>• <b>UDP</b> - User Datagram Protocol</li> </ul>
Domain	Provide the domain name.
Persistent TCP Connection	If enabled, it will not close the TCP connection on the iteration end.
Enable IPsec	Select this option to enable IPSEC.
Registration Refresh Time	Select whether to use a <b>Negotiated</b> refresh time, or a <b>Custom</b> type: <ul style="list-style-type: none"> <li>• <b>Negotiated</b> - the registration refresh will be sent after 50% of the expiration time received in <b>200 OK</b> response.</li> <li>• <b>Custom</b> - allows you to set the registration refresh interval</li> </ul>
Custom Registration Refresh Interval (s)	This parameter appears only if <b>Registration Refresh Time</b> is set to <b>Custom</b> . The time interval (in seconds) to send SIP Registration Refresh.
Number of Loops after Registration to Send Deregistration	This parameter will send the SIP Deregister at the end of each configured iteration number.
Advanced SIP Settings	For more details about these settings, refer to <a href="#">Advanced SIP Settings</a> .
<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.

Parameter	Description
Enable RTCP	Select this option in order to enable Real-Time Transport Control Protocol (RTCP).
Enable SRTP	Select this option in order to enable Secure Real-time Transport Protocol (SRTP).
RTP Session Duration (ms)	Set the value for the session duration.
<i>Audio settings:</i>	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
<i>Video Settings:</i>	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
<i>MSRP Settings:</i>	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
<i>MCTTP Settings</i>	<i>For the configuration of MCTTP settings, refer to <a href="#">MCPTT Settings</a>.</i>
<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"> <li>• <b>None</b></li> <li>• <b>EVS/AMR IPv4</b></li> <li>• <b>NB Codecs IPv6</b></li> <li>• <b>AMR-WB IPv6</b></li> <li>• <b>Multimedia IPv4</b></li> </ul>
<i>QoE Settings</i>	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

## Flow Editor

Press  to open the editor's window. The following settings are available:

Parameter	Description
Procedures Library	<p><b>TIP</b> This library can also be accessed from Test Overview &gt; Procedures Library, while the procedures are managed from the <a href="#">Settings &gt; Resource Library</a>.</p> <p>Select to access the Procedures Library, where you will find the following categories:</p> <ul style="list-style-type: none"> <li>• <b>SIP</b> - will include the procedures related to SIP signaling.</li> <li>• <b>Media</b> - will includethe procedures related to media (audio or/and video)</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>Flow</b> - will include the Start and Stop procedures used to define an iteration. The number of iterations can be configured per each UE range on the Voice objective, Dial Plan section (0 meaning infinite loops).</li> </ul> <p>See <a href="#">Procedures Library</a> for more information.</p>
Current Range	This field will be automatically populated with the name of the UE range on which the Voice application traffic is configured.
Add required procedures first > Procedures	Add the procedures required for this custom flow.
Linked Range	Select from the drop-down the UE range that will be connected. Then, add the procedures corresponding to the configuration of state machine.

Note that every procedure added under the Procedures list includes an **Add +** button and an **Expand** button:

- Use the Expand button to see the **Next On Success** and **Next on Error** configuration fields for the respective procedure. Proceed on setting up these fields for each procedure added.
- Use the **Add** button to add more steps to the procedure. Set the procedures as above.
- The red connections that appear between procedures will let you know how these are connected.

See also the [Procedures Resources \(SIP/Media/Flow\)](#) section for complete information on:

- [procedures resources and their management](#)
- [adding predefined procedures](#) from the Resource Library
- [using the Flow Editor](#) and other configurations required
- [creating a procedure from scratch](#)

## Dial Plan

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

Parameter	Description
Destination IP	The destination IP address.
Destination IP Increment	The value by which the destination IP is incremented.
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
MCC	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.

Parameter	Description
MSIN	<p>The MSIN value that will be assigned to the first simulated UE in the range.</p> <p><b>About MSIN ...</b></p> <p>The Mobile Subscriber Identification Number (MSIN) is a number that a wireless operator uses to uniquely identify a mobile phone. It is—at most—10-digits long. The MSIN is used (in combination with the MCC and MNC) to form the International Mobile Subscriber Identity (IMSI) number.</p>
IMSI Phone Increment	The value by which the IMSI phone number is incremented.
Destination Phone	The destination phone number.
Destination Phone Increment	The value by which the destination phone number is incremented.
Source Phone	The source phone number.
Source Phone Increment	The value by which the destination phone number is incremented.
Destination Port	The destination port number.

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Voice	Select the QoS flow used for voice 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:

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>AMR</b> - 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.</li> <li>• <b>AMR-WB</b> - 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.</li> <li>• <b>EVS</b> - 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.</li> <li>• <b>PCMU</b></li> <li>• <b>PCMA</b></li> <li>• <b>iLBC</b></li> <li>• <b>G722</b></li> <li>• <b>G723</b></li> <li>• <b>G729</b></li> </ul> <p>The parameters of each audio codec are presented below.</p>

### AMR/AMR-WB

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

**EVS**

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet.
Payload Type	Specifies the audio payload type.
Payload Format	The following options are available: <ul style="list-style-type: none"> <li><b>Full header</b> - 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.</li> <li><b>Compact</b> - 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.</li> </ul>
Bitrate	Indicates the mode(bitrate) of the EVS codec. Select the value from the drop-down list.

**PCMU/PCMA/iLBC/G722/G723/G729**

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

**Video Settings**

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Video	Select the QoS Flows ID(s) from the drop-down list.
Video Codecs	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.

Parameter	Description
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

## MSRP Settings

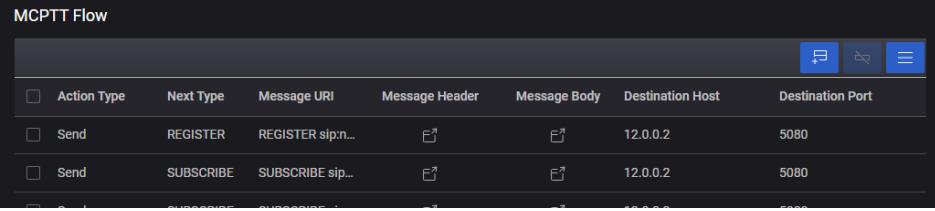
The parameters required for MSRP settings are presented in the table below.

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

## MCPTT Settings

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

Parameter	Description
Enable MCPTT	Select to enable this option.
QoS Flow ID for MCPTT	Select the QoS Flows ID(s) from the drop-down list.
MCPTT Message Format	The MCPTT message format defined according to TS 24.380 standard.
MCPTT Group	The first MCPTT Group ID.
MCPTT Group Size	The number of participants per MCPTT group call.
Use CRLF in flow csv	If enabled, it will use the CRLF line terminator in the generated CSV of the configured MCPTT flow. If disabled, it will use LF.
MCPTT Flow 	Press the <b>Open MCPTT Flow Editor</b> button to open the configuration page. Use the <b>Add New Row</b> button, and then select each column field to edit the flow.

Parameter	Description
	

## 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

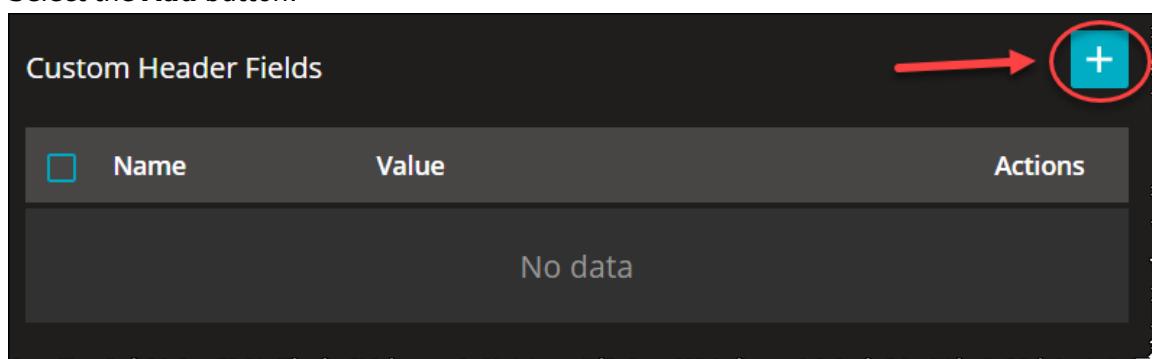
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

**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:

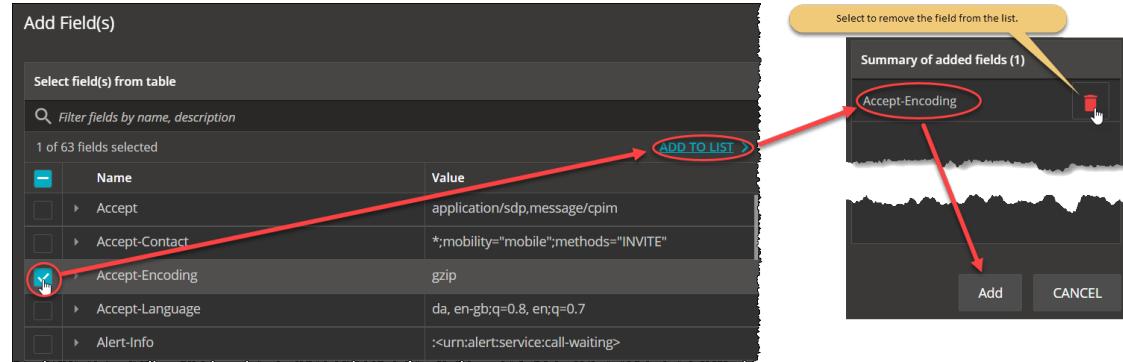
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
  - Select the **Add** button.



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, IETF RFC 3310	nextnonce="47364c23432d2e131a5fb210812c"

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
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 3261	3600
Feature-Caps	IETF RFC	+3gpp.trf=sip:trf3.operator3.com

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
	6809, 3GPP TS 24.229	
Geolocation	IETF RFC 6442	<user1@operator1.com>
In-Reply-To	IETF RFC 3261	70710@saturn.bell-tel.com, 17320@saturn.bell-tel.com
Max-Forwards	IETF RFC 3261	70
MIME-Version	IETF RFC 3261	1.0
Min-Expires	IETF RFC 3261	40
Min-SE	IETF RFC 4028	60
Organization	IETF RFC 3261	Keysight
P-Access-Network-Info	IETF RFC 7315	3GPP-E-UTRAN-FDD;e-utran-cell-id-3gpp=1234
P-Associated-URI	IETF RFC 7315	sip:user2@operator3.com
Path	IETF RFC 3327	<sip:P2.example.com;lr>,<sip:P1.example.com;lr>
P-Called-Party-ID	IETF RFC	sip:user1-business@example.com

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
	7315	
P-Chargin g-Function-Addresse s	IETF RFC 7315	ccf=192.0.8.1; ecf=192.0.8.3
P-Chargin g-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
Permissi on-Missing	IETF RFC 5360	userC@example.com
P-Preferre d-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferre d-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmtel
Priority	IETF RFC 3261	emergency
Proxy-Authenti cate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=False,algorithm=MD5
Proxy-Authoriz ation	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-	IETF	Visited network number 1

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
Visited-Network-ID	RFC 7315	
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

Parameter	Description	Value
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
Timestamp	IETF RFC 3261	Timestamp
Unsupported	IETF RFC 3261	100Rel
User-Agent	IETF RFC 3261	LoadCore
Warning	IETF RFC 3261	307 isi.edu "Session parameter `foo` not understood"

## SIP Authentication

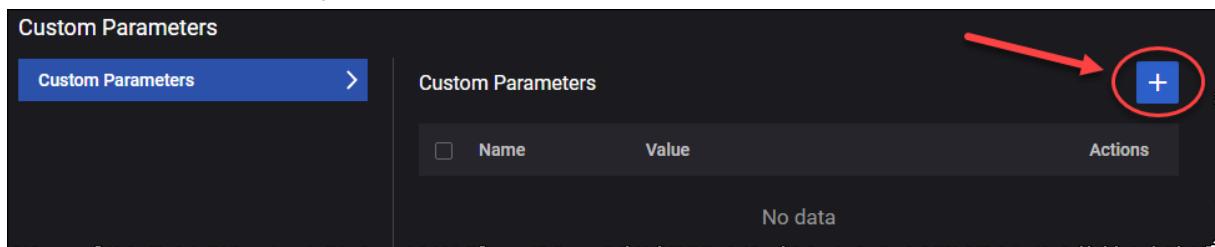
The parameters required for SIP authentication are presented in the table below.

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

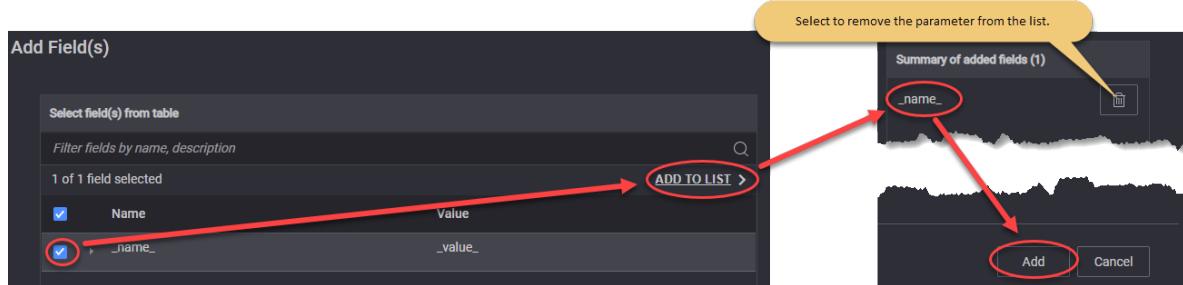
1. The Custom Parameters panel, select the **Add** button.



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 miliseconds for any SIP message. Default is set to standard 32000ms. Use this parameter to modify the default value.	32000
MaxActiveLimit	Set maximum allowed concurrent TCP connections per CPU Core. Default it is set to 8000. Please use this parameter to modify the default value.	8000

### SIP 3GPP IPSEC

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

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

### 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 <b>Video OTT</b> .
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: <b>Simulated Users</b> or <b>Throughput</b> .
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: <b>IPv4</b> or <b>IPv6</b> .
Advanced OTT	Select the <b>Open Advanced OTT</b> button to enable and configure <a href="#">Advanced OTT Settings</a> .

## 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"> <li>To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul>
<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"> <li><b>DASH</b></li> <li><b>HLS</b></li> </ul>
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 <b>Play duration</b> field is disabled and the original

Parameter	Description
	playtime is used.
Play Duration (sec)	This field is available only if the <b>Play Until End</b> 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"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Quality Control</a> pane.
Advanced Client settings	These settings are presented in the <a href="#">Advanced Client Settings</a> 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: <b>Disabled</b> or <b>Mode 0</b> .
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Adaptive Bit Rate</b></li> <li>• <b>Quality Predefined Levels</b></li> <li>• <b>Lowest Quality</b></li> <li>• <b>Highest Quality</b></li> </ul>
Number of segments	This field is available and editable only when the Quality Control Mode is set to <b>Adaptive Bit Rate</b> .
<i>Play Profiles:</i> The following settings are available and editable only when the Quality Control Mode is set to <b>Quality Predefined Levels</b> .	

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"> <li>• <b>Stay at Current Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lower Bitrate</b></li> <li>• <b>Change to the Higher Bitrate</b></li> </ul>
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to <b>Change to Higher Bitrate</b> or <b>Change to Lower Bitrate</b> .
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

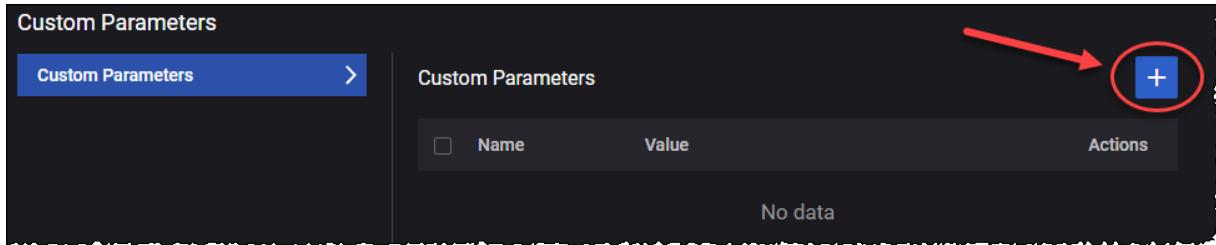
The parameters required for Advanced Client settings are presented in the table below.

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 <a href="#">Custom parameters</a> .

## Custom Parameters

You can add custom parameters as follows:

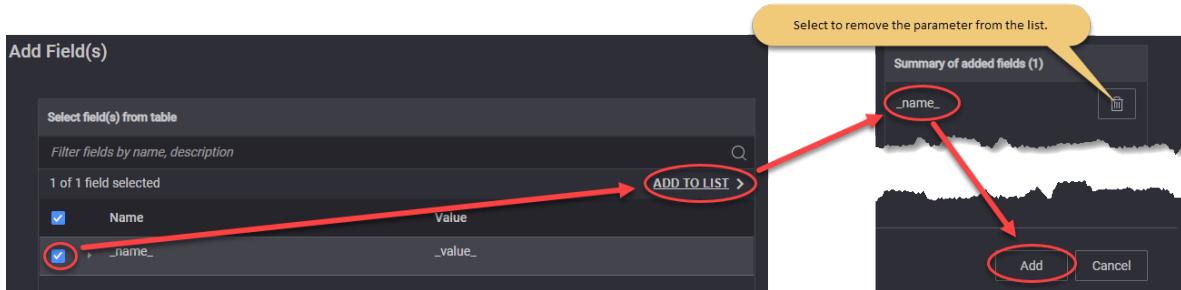
1. Select the **Open Custom Parameters** tile. The Custom Parameters panel opens.
2. Select the **Add** button.



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 <b>DNS Client</b> .
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 <b>Simulated Users</b> 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>

<b>Parameter</b>	<b>Description</b>
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: <b>IPv4</b> or <b>IPv6</b> .
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"> <li>• To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>• To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul> <p>Refer to <a href="#">Flow</a> or a description of the configuration settings for these traffic flows. Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Flow</b> button to remove the flow from your configuration.
Type	By default, the type is set to <b>DNS Client</b> .
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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
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

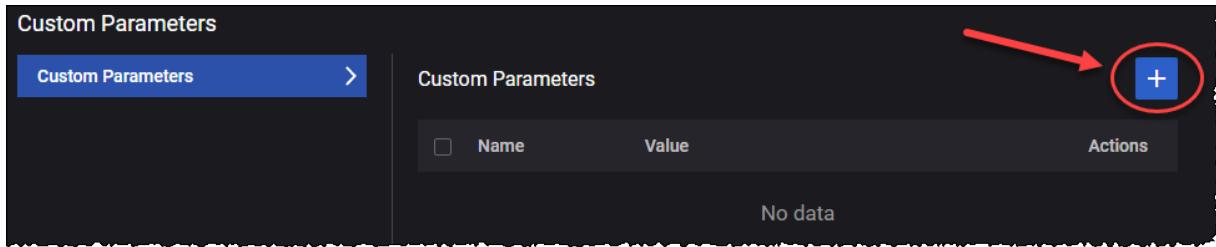
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

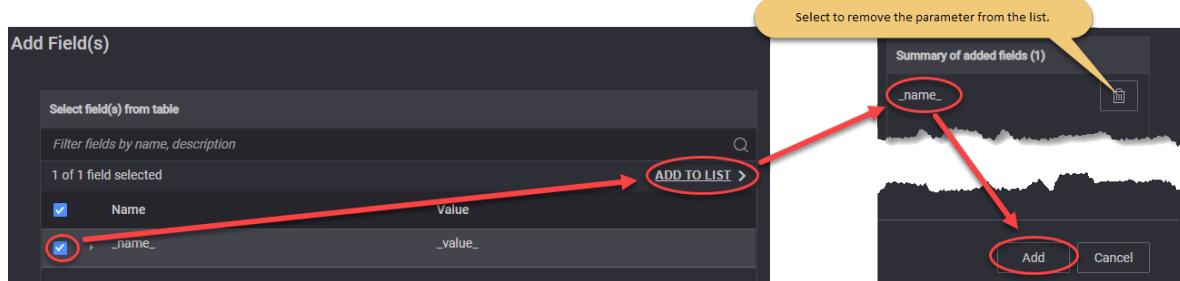
2. Select the **Add** button.



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 <b>ICMP Client</b> .
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 <b>Simulated Users</b> 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: <b>IPv4</b> or <b>IPv6</b> .
Traffic Flow	Refer to <a href="#">Traffic Flow</a> 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.

## 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 <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b>

Parameter	Description
	(option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (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"> <li>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.</li> <li>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).</li> </ul> <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: <b>Initiator</b> and <b>Responder</b> . Default value: <b>Initiator</b> .

Parameter	Description
Filter Expression	This field cannot be empty. It selects the packets to be replayed from uploaded capture. The filter string should be in <code>pcap-filter</code> format, as described at <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> (option disabled).
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to <b>Initiator</b> . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

## Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>Synthetic</b> .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be 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: <b>IPv4</b> or <b>IPv6</b> .

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

<b>Parameter</b>	<b>Description</b>
	number).

The following table describes the Traffic Flow parameters.

<b>Parameter</b>	<b>Description</b>
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Client Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
Server Burst Interval	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
Server Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

## UDG

The following table describes the UDG parameters.

<b>Parameter</b>	<b>Description</b>
Application Type	Select the application type. In this case, this parameter must be set to

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

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

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

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>UDP</b> .
<i>Out of Band Signaling</i>	Select this check-box to enable OOB signaling. More details about the required parameters <a href="#">here</a> . <b>IMPORTANT</b> To use the OOB feature, the OOB interface must be set in Agent Management window.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Source Port	The local port for client data connection.
Reconnect Timeout (ms)	The time interval after which the client attempts to reconnect after the connection was interrupted. 0 means that reconnect is disabled.
DNN	Select the DNN from the drop-down list.

Parameter	Description
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
<i>UDG Traffic Parameters</i>	<i>Select to enable and configure the <a href="#">UDG Traffic Parameters</a>.</i>
<i>Transaction</i>	<i>Select to enable and configure the <a href="#">Transaction</a> parameters.</i>
Status Query Interval	Timeout for keepalive packets on server. The server will wait for the <code>keepAliveInterval</code> value multiplied by <code>keepAliveExpiryCount</code> value.
Keepalive Interval	The time interval, in milliseconds, between UDG statistics requests (RESULT). A zero value means this feature is disabled.
Keepalive Expiry Count	The time to wait for UUDG to reconnect. A 0 value means the reconnect is disabled (in milliseconds).

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

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

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

Parameter	Description
UDG Test Type	Select the test type from the drop-down list. Available options: <b>Transmission</b> , <b>Ping-pong</b> or <b>Speed-Test</b> . For each test type, the parameters are described below.
<i>Transmission</i>	
Throughput Tx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change.

Parameter	Description
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Interval Unit	The unit in which this burst interval is expressed.
Client Burst Size (packets)	The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Throughput Rx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change. A corresponding server is required to achieve the displayed value.
Server Burst Interval (ms)	The time interval at which the server sends packet bursts.
Server Burst Interval Unit	The unit in which this burst interval is expressed.
Server Burst Size (packets)	The number of packets the server sends in a burst.
Server Burst Interval Unit	Select the server burst interval unit. Available options: <b>Millisecond</b> or <b>Microsecond</b> .
Server Burst Size (bytes)	The packet size in bytes.
<i>Ping-pong</i>	
Ping Direction	Set the ping direction. Available options: <b>Upstream</b> or <b>Downstream</b> .
Ping Interval	Set the ping time interval.
Ping Interval Unit	Set the ping interval unit. Available options: <b>Millisecond</b> or <b>Microsecond</b> .
Pong Number	Set the value for the pong number.
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.
<i>Speed-Test</i>	
Traffic direction	Select the traffic direction for which this filter applies: <b>Uplink</b> or <b>Downlink</b> .

Parameter	Description
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.

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

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

## REST API Client

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

The following table describes the REST API Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>REST API Client</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	This field is set to <b>Simulated Users</b> and cannot be modified.
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>TLS</b>
REST API Flow	The name of list of REST API Client sequential operations and transitions emulated by each REST API Client.  The REST API Flow is initially loaded into LoadCore's Resource Library, and then added to the test as a <a href="#">Global Playlists</a> . The list is defined in CSV format, following specific rules. Refer to <a href="#">Work with the Resource Library on page 73</a> section for further information.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before starting the Attacks objective traffic.

Parameter	Description
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .
Iterations	If is set to <b>0</b> , it will be iterated on continuous loop during sustain time. If set to <b>1</b> , it will be executed only one time. <b>IMPORTANT</b> Values greater than 1 are not allowed.
Max Transactions per Connection	The maximum amount of transactions an application can make on one connection.
Enable DNS Query per Connection	If enabled, will process only one DNS query per TCP connection.
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes. The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional

Parameter	Description
	Ethernet, the MSS value is 1460 (1500 minus 40).
Selective Acknowledgments	Select the toggle button to enable this option.
Custom Parameters	For more details, refer to <a href="#">Custom parameters</a> .

## Custom Parameters

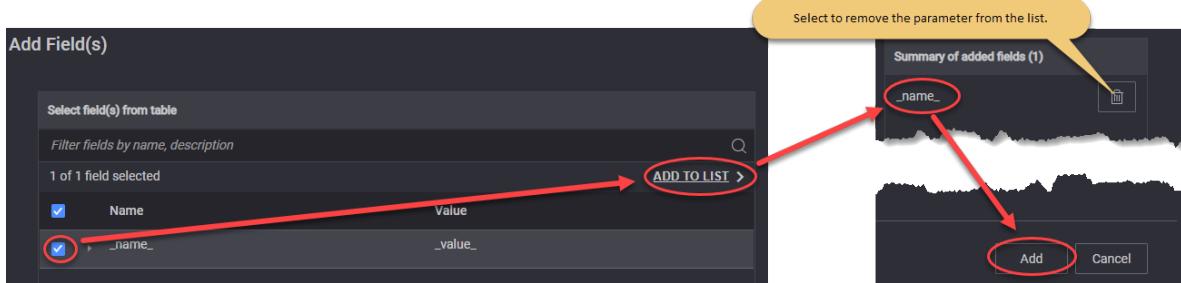
From this section you can add custom parameters fields:

- **Custom Parameters**

You can add custom parameters as follows:

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

**For example ...**



## How to Configure the REST API Client

1. Define your REST API flow in an CSV file, following the rules described in the [REST Client Flow specifications](#).
2. Load the CSV as a Global Playlist in LoadCore user interface:
  - a. Go to **Global Settings > Global Playlist**.
  - b. Add a new Playlist using the **+** button.
  - c. **Name** the new Playlist - it will be used in the REST API Client application configuration.
  - d. **Upload** the CSV created at **Step 1**.
3. In the User Plane UE section, select the **REST API Client** application traffic.
4. Set all necessary parameters on required by the application (see [REST API parameters table](#) above):
  - on **Transport protocol** select **TCP** or **TLS** (version 1.2 and 1.3 configurable from TLS Settings).
  - the **Objective type** is automatically set to **Simulated users**.

- add the **REST API Flow** name that defines the REST sequence of actions defined in the Global Playlist.
- set the **Max Transactions per Connection**- for REST API Client application, one "Transaction" points to all REST actions (HTTP requests) specified in REST flow.
- Set all other common parameters.

## REST Client Flow specifications

The REST Client flow will be specified in CSV format state-by-state. For each State in flow, three main commands must be specified, and one special command at the end of list:

Command	Condition	Description
<b>Action</b>	Mandatory	<p>Indicates what actions should be executed in the current State and what transitions can be executed. The following rules are in place:</p> <ul style="list-style-type: none"> <li>• up to 4 transitions are allowed. Maximum 4 pairs of (Conditions, NextState) are used from CSV.</li> <li>• Method, Headers and Body should be specified in separate columns.</li> <li>• Method, Headers and Body can contain dynamic parts specified by flow user variables.</li> </ul>
<b>Extract</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>Specifies if some elements from the last HTTP response should be extracted in user variables for further utilization in flow:</p> <ul style="list-style-type: none"> <li>• extractions are specified using (backqoute_separated_path, userVar) pairs.</li> <li>• up to 3 extractions per REST(HTTP) response are allowed.</li> </ul>
<b>Statistics</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>User-defined Counters can be incremented when the condition is fulfilled. The configuration is done in pairs of (condition, UserCounter).</p>
<b>ENDMARKER</b>	Mandatory	This special command is mandatory to indicate the end of REST API flow. No other command will be executed after the ENDMARKER was executed. It can be inserted anywhere in the Playlist, on the first column.

## REST user flow variables

There are 10 flow variables with predefined names (userVar1, userVar2,...,userVar10) available for store extracted values from REST Commands during flow duration. On each REST Command, you can configure what to extract from the received Response, and in what variable.

Each variable can be overwritten at anytime, therefore a variable can be persistent during the flow duration, or only temporary, until overwrite.

## Predefined Applications Traffic

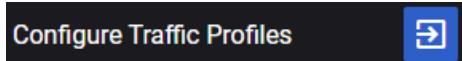
The following table describes the Predefined Flows Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Predefined Applications</b> .
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"> <li>• <b>Simulated Users</b></li> <li>• <b>Throughput</b></li> <li>• <b>Connections Per Second</b></li> </ul>
Throughput (kbps)	<p><b>IMPORTANT</b> This parameter is available only when <a href="#">Objective Type</a> is set to <b>Throughput</b>.</p> <p>The desired throughput (in kbps) for the combined traffic flows that will be generated.</p>
Connections Per Seconds	<p><b>IMPORTANT</b> This parameter is available only when <a href="#">Objective Type</a> is set to <b>Connections Per Second</b>.</p> <p>Set the number of connections.</p>
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size 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.
Configure Traffic Profiles	<p>Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions.</p> <p>Refer to <a href="#">Traffic Profile</a> for a description of the configuration settings for these traffic profiles.</p>

## Traffic Profile

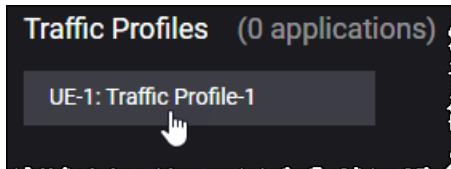
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

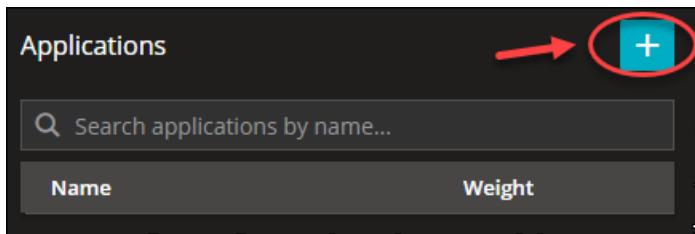
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

## Applications

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

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



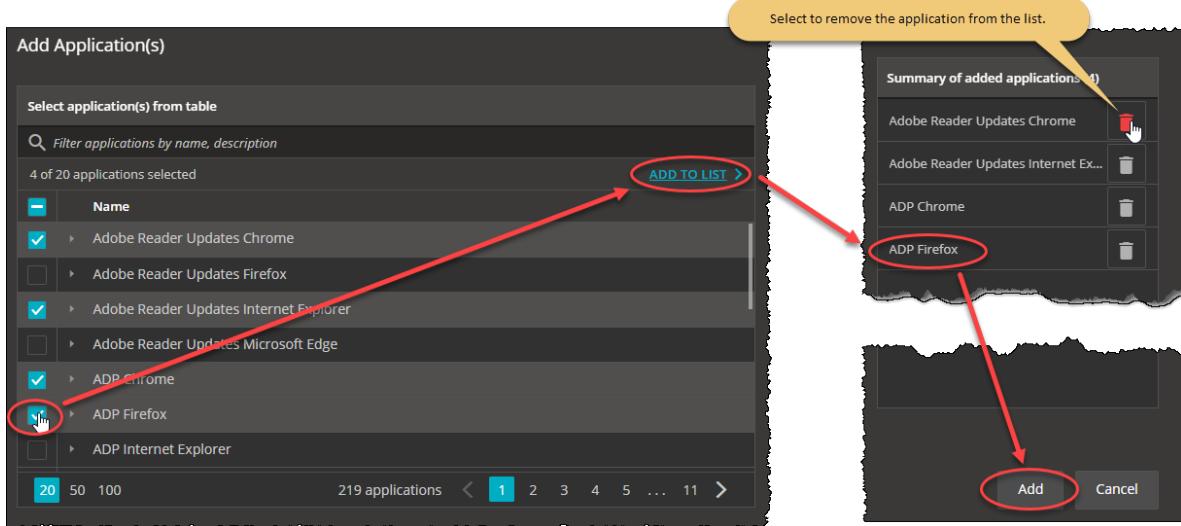
The Add Application(s) window opens.

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

**NOTE**

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

**For example ...**



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

**For example ...**

Name	Weight	Action
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 <b>Throughput</b> , 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"> <li>• <b>Rename</b> - Select to rename the application.</li> <li>• <b>Advanced Settings</b> - for more information, refer to <a href="#">Advanced Settings</a>.</li> <li>• <b>Delete</b> - Select to delete the application.</li> </ul>

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

### For example ...

The screenshot shows the LoadCore application management interface. On the left, there is a list of predefined applications with columns for Name and Weight. One application, "Adobe Reader Updates Chrome 1", is selected and highlighted with a cursor. To the right, the "Application Settings" section is displayed, containing fields for Destination Hostname, DNN ID, and QoS Flow ID. Below this, the "Application Actions" section is shown, listing actions such as "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.

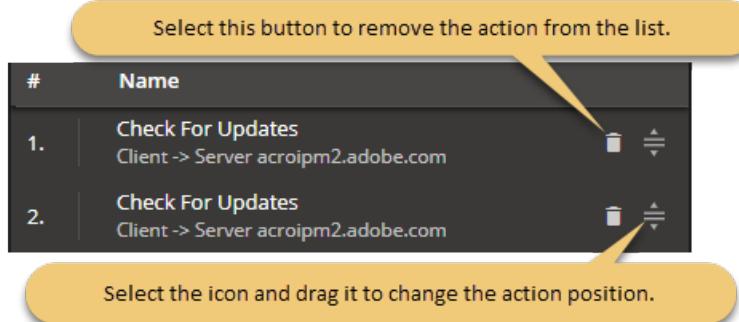
### Application Actions

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.

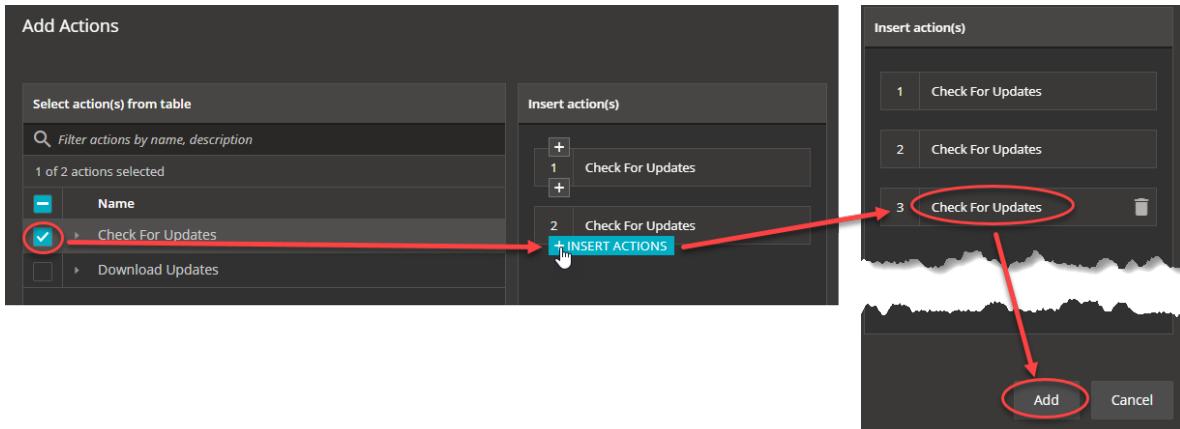
### For example ...



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 ...**



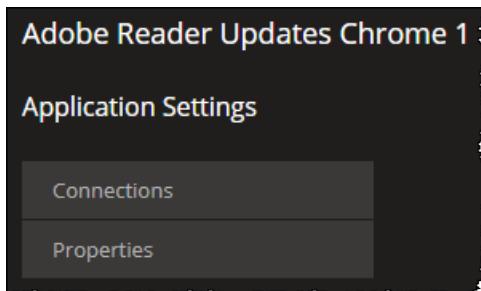
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

## 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.

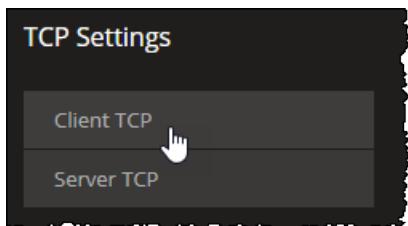
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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"> <li>• Chrome</li> <li>• Firefox</li> <li>• Opera</li> <li>• Microsoft Edge</li> <li>• Internet Explorer</li> <li>• Safari</li> <li>• Android</li> </ul>
Action Timeout (seconds)	Set the action timeout in seconds.
Connection Persistence	Select an option for the connection persistence: <ul style="list-style-type: none"> <li>• <b>Standard</b> - inherits the behavior with respect to the HTTP version (1.0 or 1.1).</li> <li>• <b>Disabled</b> - enforces connection closing following every HTTP message.</li> <li>• <b>Enabled</b> - enforces connection persistence through explicit keep-alive.</li> </ul>

Field	Description
HTTP Version	Select the HTTP version used: <ul style="list-style-type: none"> <li>• <b>HTTP/1.0</b></li> <li>• <b>HTTP/1.1</b></li> </ul>

## TCP Settings

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



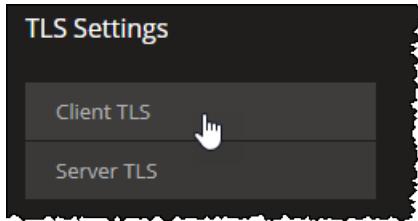
These parameters are configurable for both Client and Server settings, as presented in the following table.

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 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.

Parameter	Description
Enable RFC1323 TCP timestamps	<p>Enable or disable the stamp using the toggle button. If enabled, the client or server inserts an RFC 1323 timestamp into each packet.</p> <p><b>NOTE</b> 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
<i>TLSv1.2</i>	<p>Select the check box to enable it. The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Disable</li> <li>• Session ticket</li> <li>• Session ID</li> </ul> <p><b>NOTE</b> Session reuse method is available only if <i>TLSv1.2</i> is selected.</p>

Parameter	Description
Immediate close	Select the check box to enable it.
TLSv1.3	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	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	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Disable</li> <li>• Session ticket</li> <li>• Session ID</li> </ul> <p><b>NOTE</b> Session reuse method is available only if TLSv1.2 is selected.</p>
Immediate close	Select the check box to enable it.
TLSv1.3	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	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.
SNI Enabled	<i>Select the check box to enable the server name indicator. The following <b>SNI Settings</b> become available:</i>
Certificate file	Select <b>Upload</b> to add your certificate file or <b>Clear</b> to remove it.

Parameter	Description
Key file	Select <b>Upload</b> to add your key file or <b>Clear</b> to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select <b>Upload</b> to add your DH file or <b>Clear</b> to remove it.
<i>Certificate file</i>	<i>Select <b>Upload</b> to add your certificate file or <b>Clear</b> to remove it.</i>
<i>Key file</i>	<i>Select <b>Upload</b> to add your key file or <b>Clear</b> to remove it.</i>
<i>Key file password</i>	<i>Enter your key file password.</i>
<i>DH file Traffic</i>	<i>Select <b>Upload</b> to add your DH file or <b>Clear</b> 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: <b>None</b> , <b>XOR</b> , <b>ZOOM</b> or <b>SRTP</b> .
MOS Mode	Select the Session Reuse Method from the drop-down list. Available options: <b>Disable</b> , <b>Per interval</b> or <b>Per call</b> .

## 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:

<b>RAN Ranges panel</b> .....	<b>852</b>
<b>RAN Range settings</b> .....	<b>852</b>
<b>RAN N3 interface settings</b> .....	<b>853</b>
<b>Passthrough interface settings</b> .....	<b>854</b>

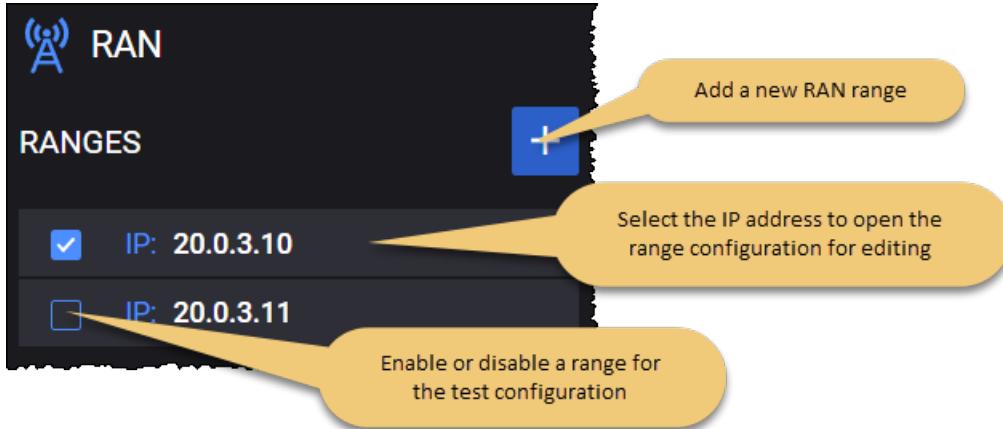
## RAN Ranges panel

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 <b>Delete Range</b> 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 <a href="#">RAN N3 interface settings</a> .
Passthrough Interface Settings	These settings are described in <a href="#">passthrough interface settings</a> .

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

<b>Connectivity Settings</b>	<b>Description</b>
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.

<b>Connectivity Settings</b>	<b>Description</b>
<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	<b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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:

<b>SMF Ranges panel</b> .....	<b>856</b>
<b>SMF Range settings</b> .....	<b>856</b>
<b>SMF N4 interface settings</b> .....	<b>857</b>
<b>SMF Uplink Paths</b> .....	<b>859</b>

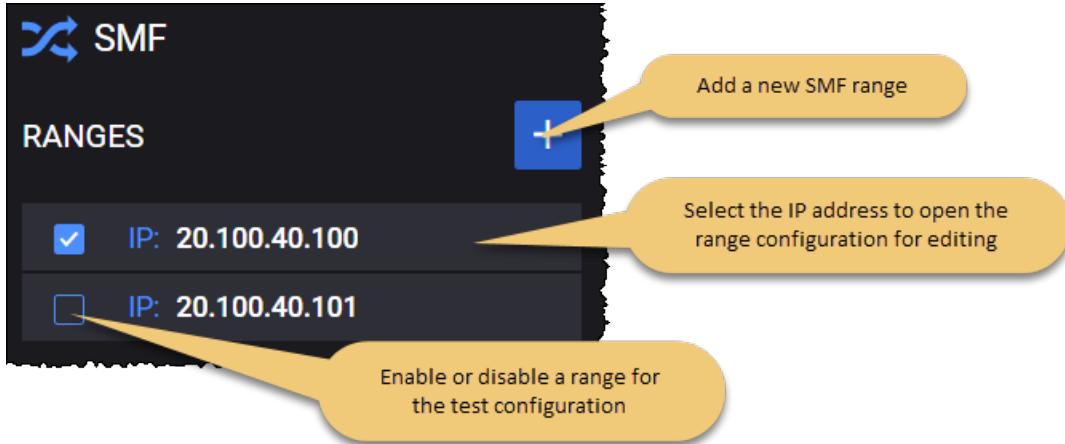
## SMF Ranges panel

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 <b>Delete Range</b> button to delete this range from your test configuration.
Name	The name uniquely identifies the SMF instance. You can accept the value provided by LoadCore or overwrite it with your own value.
<i>Range Settings:</i>	

Setting	Description
N4 Interface Settings	Each SMF range requires the configuration of N4 interface settings, through which a SMF instance interacts with UPF in a 5G network. These settings are described in <a href="#">SMF N4 interface settings</a> .
Uplink Paths	These settings are described in <a href="#">SMF uplink paths</a> .

## 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 <b>Supports FTEID Allocation</b> 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 <b>Enable N4u Interface</b> 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>	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>

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:

<b>i-UPF:</b>	one N3 UPF (I-UPF) and one N9 UPF	In this case all flows of a PDU session will use the path <i>RAN &gt; N3 UPF &gt; N9 UPF &gt; DN</i> .
<b>ULCL:</b>	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 &gt; N3 UPF &gt; First N9 UPF &gt; DN</i> , and others will use <i>RAN &gt; N3 UPF &gt; Second N9 UPF &gt; 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 <b>Add an uplink path</b> button to add an uplink path to your test configuration.
<i>Uplink Path:</i>	
	Select the <b>Delete uplink path</b> 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 <b>None</b> if your test configures only one N9 UPF or a UPF if you test configures more than one N9 UPF.

<b>Setting</b>	<b>Description</b>
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:

<b>UPF Ranges panel</b> .....	<b>862</b>
<b>UPF Range panel</b> .....	<b>862</b>
<b>UPF N3 interface settings</b> .....	<b>863</b>
<b>UPF N4 interface settings</b> .....	<b>865</b>
<b>UPF N6 interface settings</b> .....	<b>866</b>
<b>UPF N9 interface settings</b> .....	<b>867</b>
<b>UPF N4u interface settings</b> .....	<b>869</b>

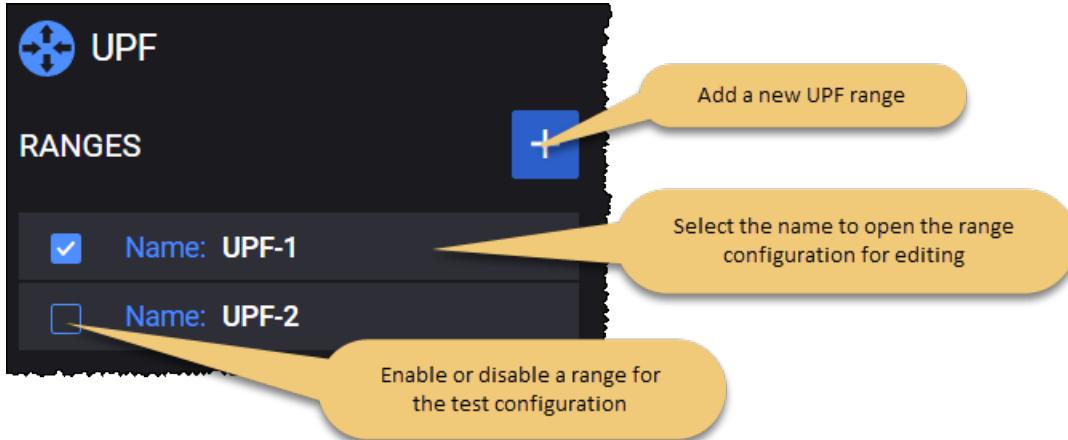
## UPF Ranges panel

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 ...**



If multiple agents are assigned to the UPF node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **All Ranges on All Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UPF node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1 and agent2, range2 on agent1 and agent2, range 3 on agent1 and agent2.
- **Round Robin Ranges on Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UPF node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1, range2 on agent2, range3 on agent1.

## 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 <b>Delete Range</b> 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.
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 <a href="#">UPF N3 interface settings</a> .
N4 Interface Settings	N4 is the interface between the SMF and the UPF. The interface settings are described in <a href="#">UPF N4 interface settings</a> .
N6 Interface Settings	N6 is the interface between the DN and the UPF. The interface settings are described in <a href="#">UPF N6 interface settings</a> .
N9 Interface Settings	N9 is the interface between two UPFs. The interface settings are described in <a href="#">UPF N9 interface settings</a> .
N4u Interface Settings	N4u is an interface between the SMF and the UPF. The interface settings are described in <a href="#">UPF N4u interface settings</a> .

## 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 <b>Add value</b> button to add a network instance to your test configuration.

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

## UPF N4 interface settings

The UPF receives user traffic information from the SMF over the N4 interface. N4—which employs the Packet Forwarding Control Protocol (PFCP)—is the control plane interface between the UPF and the SMF. PFCP sessions established with the UPF define how packets are identified, forwarded, processed, marked, and reported (using PDRs, FARs, BARs, QERs, and URRs).

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

Setting	Description
<i>N4 Interface Settings:</i>	
Peer SMF	<p>By default, the value is set to <b>None</b>. 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 <b>Supports FTEID Allocation</b> 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
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	The IP address assigned as gateway address.

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

## 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.

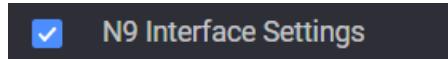
<b>Connectivity Settings</b>	<b>Description</b>
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number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

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

## 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:



<b>Interface Settings</b>	<b>Description</b>
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>	

Interface Settings	Description
	Select the <b>Add value</b> button to add a network instance to your test configuration.
	Select the <b>Delete</b> 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.
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner</i></p>

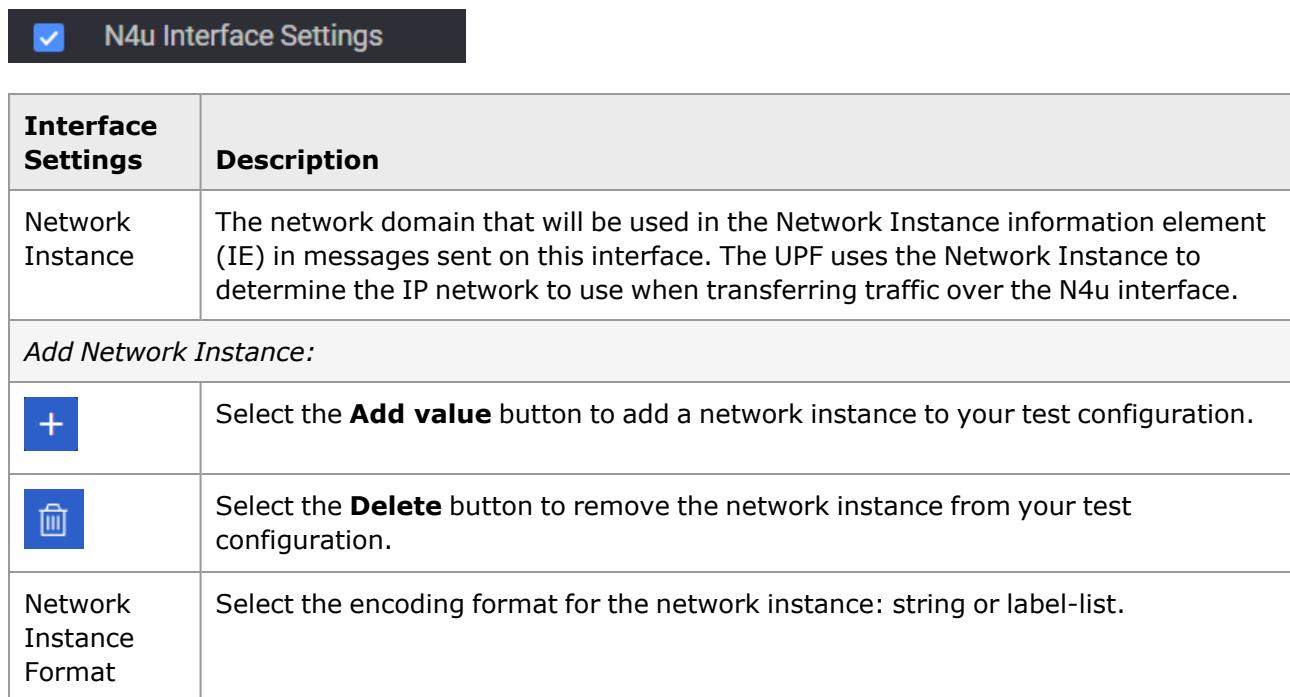
<b>Connectivity Settings</b>	<b>Description</b>
	<i>VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## 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:



<b>Interface Settings</b>	<b>Description</b>
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 <b>Add value</b> button to add a network instance to your test configuration.
	Select the <b>Delete</b> 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.

<b>Connectivity Settings</b>	<b>Description</b>
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.

<b>Connectivity Settings</b>	<b>Description</b>
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.
Enable Impairment	This option is available only when <b>Network management &gt; Network Stack</b> is configured to IxStack.
<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.
Gateway Address	The IP address assigned as 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>

<b>Connectivity Settings</b>	<b>Description</b>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

# DN configuration settings



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

The configuration settings are described in the topics listed below.

## Topics:

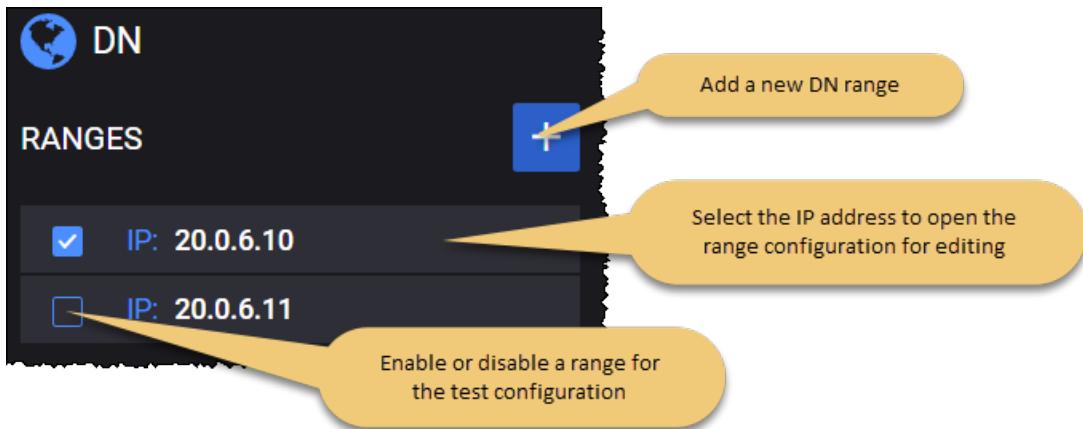
<b>DN Ranges panel</b>	<b>872</b>
<b>DN Range panel</b>	<b>873</b>
<b>DN N6 Interface settings</b>	<b>874</b>
<b>DN routes settings</b>	<b>875</b>
<b>DN User Plane</b>	<b>876</b>
DN Stateless UDP Traffic	877
DN Data Traffic	878
DN Voice Traffic	881
DN Video OTT Traffic	894
DN DNS Server Traffic	897
DN Predefined Applications Traffic	899
DN Capture Replay	899
DN Synthetic	901
DN UDG	903
<b>DN Throttling settings</b>	<b>905</b>

## 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 ...**



If multiple agents are assigned to the DN node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **All Ranges on All Agents** - influences the way configuration is distributed in case of multiple agents assigned on the DN node.

For example, for a test with 2 agents and 3 ranges: range1 on agent1 and agent2, range2 on agent1 and agent2, range 3 on agent1 and agent2.

## 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 <b>Delete Range</b> button to delete this range from your test configuration.
Range Count	The number of DNs in the DN range.
<i>Range Settings:</i>	

Setting	Description
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 <a href="#">DN N6 interface settings</a> .
Routes Settings	These settings are described in <a href="#">DN routes settings</a> .
User Plane	These settings are described in <a href="#">DN user plane</a> .
Throttling Settings	These settings are described in <a href="#">DN Throttling settings</a> .

## 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.

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

## DN routes settings

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

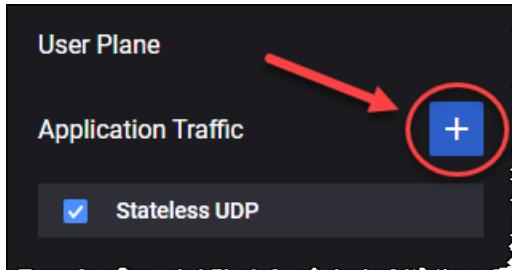
The following table describes the **Route Settings** that you need to configure in order to create the route to an UE or custom range.

Settings	Description
<i>Routes Config:</i>	
	Select this button to add a new route to a specific UE range or a custom one.
<i>UE Routes Config:</i>	
	Select this button to remove the route.
Route Type	Select the route type from the drop-down list. Available options: <b>UE</b> or <b>Custom</b> .
UE Range IPv4	Select the IPv4 address of the UE range from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .
UE Range IPv6	Select the IPv6 address of the UE range from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .
Peer UPF	Select the UPF node connected to DN over the N6 interface from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .
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 <b>Custom</b> .

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. This parameter is available only when the route type is set to <b>Custom</b> .

## 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"><li>• <b>Stateless UDP</b></li><li>• <b>Data</b></li><li>• <b>Voice</b></li><li>• <b>Video OTT</b></li><li>• <b>DNS Server</b></li><li>• <b>Predefined Applications</b></li><li>• <b>Synthetic</b></li><li>• <b>UDG</b></li></ul>
	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 <a href="#">DN Stateless UDP Traffic</a> .
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">DN Data Traffic</a> .
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">DN Voice Traffic</a> .

Parameter	Description
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">DN Video OTT Traffic</a> .
DNS Server	For the settings required to configure the DNS Server objective, refer to <a href="#">DN DNS Client Traffic</a> .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to <a href="#">DN Predefined Applications Traffic</a> .
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to <a href="#">DN Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG traffic objective, refer to <a href="#">DN UDG Traffic</a> .

## DN Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Stateless UDP</b> .
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 <b>dowlink</b> 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.

Parameter	Description
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 <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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 <b>Data</b> .
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"> <li>To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.</li> <li>To add another application server, click the <b>Add Server</b> button. LoadCore will open the Server panel where you will select the server type and configure the server settings.</li> </ul> <p>Refer to <a href="#">Server</a> (below) for a description of the configuration settings required by</p>

Parameter	Description
	<p>the application server.</p> <p>Also, you can add <a href="#"><u>custom parameters</u></a>, 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 <b>Delete Server</b> 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: <b>TCP</b> , <b>TLS</b> , <b>QUIC</b> or <b>UDP</b> .
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"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get Responder</b>, <b>HTTP Put Responder</b>, <b>HTTP Post Responder</b>, <b>HTTP Server</b> and <b>FTP Responder</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get Responder</b>, <b>HTTPS Put Responder</b>, <b>HTTPS Post Responder</b> and <b>HTTPS Server</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Server</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional Responder</b>.</li> </ul>
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. Setting the page size on DN side will only influence GET objectives, like HTTP GET, HTTPS GET and FTP. To set the page size for PUT objectives, the change must be operated on UE side.
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 <b>UDP Bidirectional</b> .
Server Tx Count	This parameter is available only when the application server type is set to <b>UDP Bidirectional</b> .

## Custom Parameters

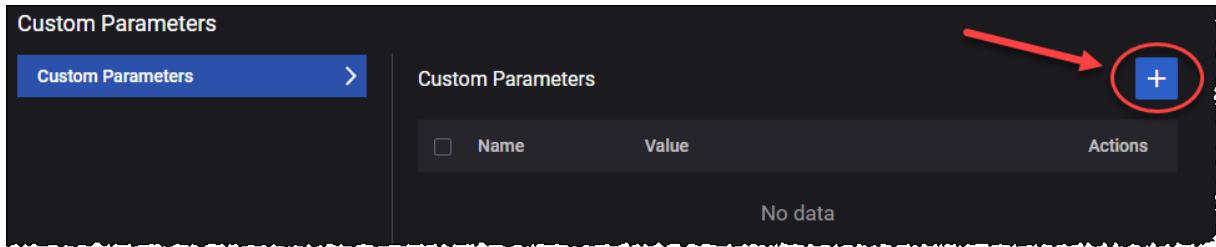
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

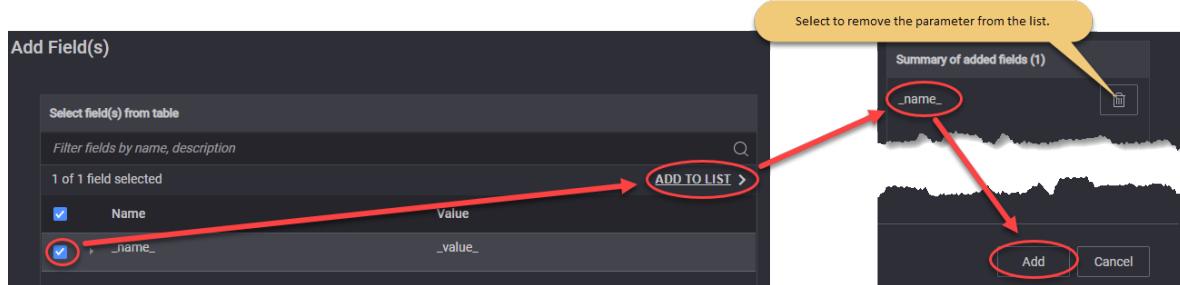
2. Select the **Add** button.



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 <b>Voice</b> .
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 <b>Simulated Users</b> and cannot be changed.
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 <a href="#">Dial Plan</a>.</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"> <li><b>TCP</b> - Transmission Control Protocol</li> <li><b>TLS</b> - Transport Layer Security</li> <li><b>UDP</b> - User Datagram Protocol</li> </ul>

Parameter	Description
Domain	Provide the domain name.
Advanced SIP Settings	For more details about these settings, refer to <a href="#">Advanced SIP Settings</a> .
<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.
Enable SRTP	Select this option in order to enable Secure Real-time Transport Protocol (SRTP).
RTP Session Duration (ms)	Set the value for the session duration.
Audio settings:	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
Video Settings:	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
MSRP Settings:	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
MCTTP Settings	<i>For the configuration of MCTTP settings, refer to <a href="#">MCPTT Settings</a>.</i>
<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"> <li>• <b>None</b></li> <li>• <b>EVS/AMR IPv4</b></li> <li>• <b>NB Codecs IPv6</b></li> <li>• <b>AMR-WB IPv6</b></li> <li>• <b>Multimedia IPv4</b></li> </ul>
QoE Settings	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

## Dial Plan

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

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

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Voice	Select the QoS flow used for voice 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"> <li>• <b>AMR</b> - 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.</li> <li>• <b>AMR-WB</b> - 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.</li> <li>• <b>EVS</b> - 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.</li> <li>• <b>PCMU</b></li> <li>• <b>PCMA</b></li> <li>• <b>iLBC</b></li> </ul>

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

### AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth efficient:</b> In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added.</li> <li>• <b>Octet aligned:</b> 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.</li> </ul>
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"> <li>• <b>Full header</b> - 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.</li> <li>• <b>Compact</b> - In this payload format a single codec data frame is sent in each RTP packet. The format uses protected payload sizes that uniquely identify</li> </ul>

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

### PCMU/PCMA/iLBC/G722/G723/G729

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

### Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Voice	Select the QoS Flows ID(s) from the drop-down list.
Video Codecs	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

### MSRP Settings

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

Parameter	Description
Enable MSRP	Select to enable this option.

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

## MCPTT Settings

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

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

## Advanced SIP Settings

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

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

### SIP Custom Headers

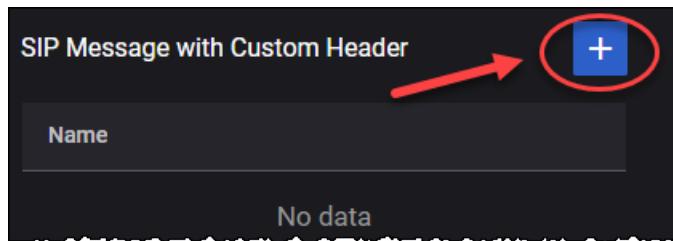
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

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

For each message, you can:

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

- Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**

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	:<urn:alert:service:call-waiting>
Allow	IETF	INVITE, ACK, UPDATE, PRACK, CANCEL, PUBLISH, ME...

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	:<urn:alert:service:call-waiting>

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

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

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

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

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

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

## SIP Authentication

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

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

Parameter	Description
	for the UEs in this range. It is a string with a maximum length of 34 characters. It remains fix for all Subscriber/SIM of an operator. You can accept the value generated by 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 <b>Video OTT</b> .
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).

### OTT Servers:

	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"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
Port	Set the port number. You can accept the value provided by LoadCore or overwrite it with your own value.

Parameter	Description
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
Streams	Refer to <a href="#">Streams</a> (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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"> <li>• <b>Real</b></li> <li>• <b>Synthetic</b></li> </ul>
Protocol	Select the protocol from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Apple HLS</b></li> <li>• <b>DASH</b>.</li> </ul> If the stream type is set to <b>Synthetic</b> , you can choose one protocol from list. If the stream type is set to <b>Real</b> , you will see the protocol of real stream loaded.
Stream Duration	If the stream type is set to <b>Synthetic</b> , you can configure the stream duration in seconds. If the stream type is set to <b>Real</b> , you will see the real stream duration.
Segment Duration	If the stream type is set to <b>Synthetic</b> , you can configure the segment duration in seconds. If the stream type is set to <b>Real</b> , you will see the real segment duration.
Quality	Set the quality value for each level.

Parameter	Description
Levels:	
	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: <b>QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K</b> .
Frames per second	Set the number of frames per second.

## Custom Parameters

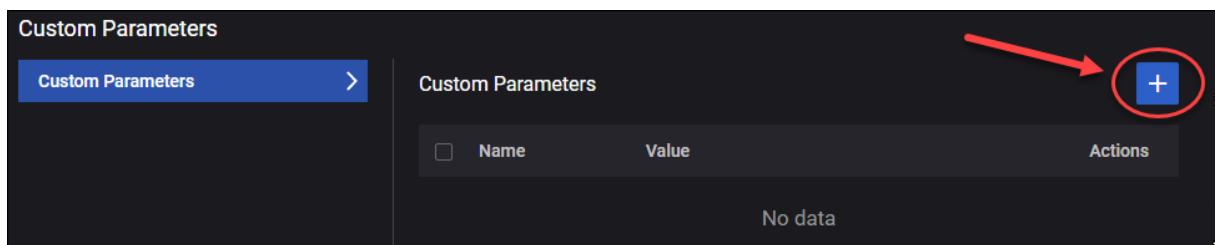
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

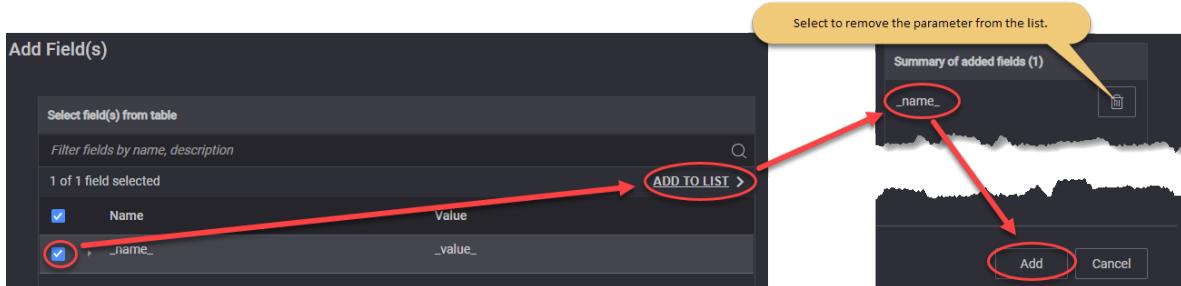
2. Select the **Add** button.



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 <b>DNS Server</b> .
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.
	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 <a href="#">Zone Manager</a> (below) for descriptions of the DNS server zones settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
Hostname	Set the hostname.
Address	Provide the address.

## Custom Parameters

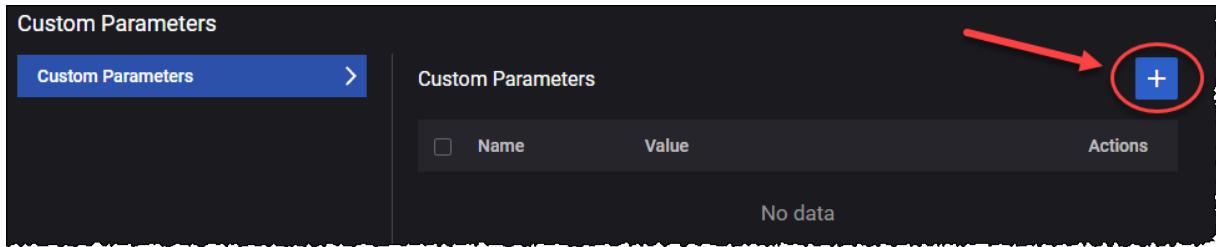
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

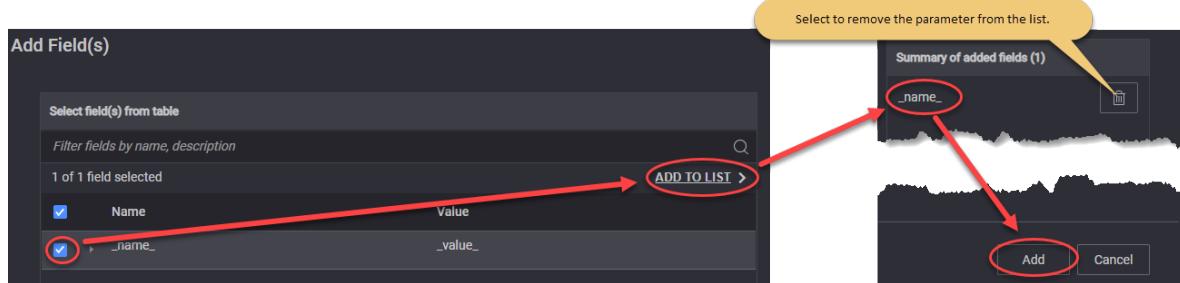
2. Select the **Add** button.



The Add Field(s) opens.

- 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 <b>Predefined Applications</b> .
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 <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b> (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (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"> <li>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.</li> <li>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).</li> </ul> <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: <b>Initiator</b> and <b>Responder</b> . Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> (option disabled).
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to <b>Initiator</b> . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

## DN Synthetic

The following table describes the Synthetic parameters.

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

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

The following table describes the Traffic Flow parameters.

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

## DN UDG

The following table describes the UDG parameters.

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

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

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

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

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

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

## DN Throttling settings

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

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

**NOTE**

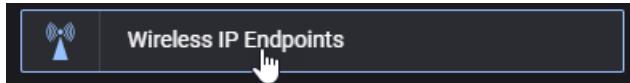
The throttling options only work for interfaces that are running IxStack, either over DPDK or over raw sockets, depending on where the traffic is terminated (if agent is present on DN/SGi server then its N6 interface should be IxStack; if there is no agent on DN/SGi, than N3 interface should be IxStack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

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

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

*CHAPTER 10***IP Endpoints tests: configuration settings**

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

**Topics:**

<b>Global Settings .....</b>	<b>909</b>
DNS Settings .....	909
Advanced Settings .....	910
UDP Buffer Settings .....	912
Impairment .....	912
Milenage .....	912
External Stats Server .....	913
Global Playlists .....	920
<b>IP Client configuration settings .....</b>	<b>922</b>
IP Client Ranges panel .....	922
IP Client Range panel .....	923
IP Client interface settings .....	924
IP Client Timeline .....	925
IP Client User Plane .....	925
Stateless UDP Traffic .....	926
Data Traffic .....	927
Voice Traffic .....	931
Video OTT Traffic .....	946
DNS Client Traffic .....	950
ICMP Client .....	953
Capture Replay .....	954
Synthetic .....	955
UDG .....	957
REST API Client .....	961
<b>Triple Play Server configuration settings .....</b>	<b>966</b>

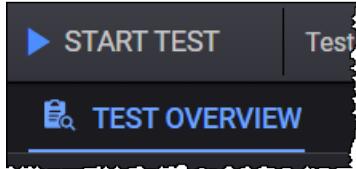
CSCF Range panel .....	966
Media Function Range panel .....	967
Data/Video configuration settings .....	968
Data/Video Ranges panel .....	969
Data/Video Range panel .....	969
Data/Video interface settings .....	970
Data/Video User Plane .....	971
Data/Video Throttling settings .....	998

## 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 access and configure the following setting:

<b>DNS Settings</b>	<b>909</b>
<b>Advanced Settings</b>	<b>910</b>
<b>UDP Buffer Settings</b>	<b>912</b>
<b>Impairment</b>	<b>912</b>
<b>Milenage</b>	<b>912</b>
<b>External Stats Server</b>	<b>913</b>
<b>Global Playlists</b>	<b>920</b>

### DNS Settings

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

The DNS information is used only for the user plane path, that is, the configured DNS Server is used to resolve the destination configured for the user plane objectives in case the destination is a host name and not an IP.

Setting	Description
<i>DNS Settings:</i>	
Cache Timeout (ms)	The amount of time (in milliseconds) the local DNS stores the address information.

Setting	Description
<i>DNS Name Servers:</i>	
	Select the <b>Add DNS Name Server</b> button to add a new DNS server to your test configuration. Set the IP address of the DNS server.
	Select the <b>Delete</b> button to remove the DNS server from your test configuration.

## Advanced Settings

The advanced settings are described in the following table:

Setting	Description
Overwrite Capture Size	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size	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.
Power Saver on Agents	Select this option to disable the IxStack/DPDK at the end of each test on all agents.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: <ul style="list-style-type: none"> <li><b>None</b> - no advanced statistics enabled.</li> <li><b>One Way Delay</b> - the time spent by the packet on the network from the moment it is sent until it is received.</li> <li><b>Delay Variation Jitter</b> - the per polling interval average delay variation jitter value calculated for all packets.</li> </ul>
Automated Polling Interval	This option is enabled by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval (sec)	This option becomes available only when <i>Automated Polling Interval</i> option is disabled. It allows you to create a custom polling interval.
Log Level	Select one of the options: <ul style="list-style-type: none"> <li><b>Info</b> - Designates informational messages that highlight the progress of the application at coarse-grained level.</li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• <b>Debug</b> - Designates fine-grained informational events that are most useful to debug the application.</li> </ul>
Log Tags	<p>Select one or more tags from the drop-down list.</p> <p>Log Tags are used to collect specific information in the logs; they work with Debug and with Info log levels. Rather than allowing the logs to collect information about everything, you can use Log Tags to collect specific information—such as SCTP or HTTP messages—during the test. This limits the amount of information that is collected, making it easier for you to extract the data that you need.</p>
Ignore Offline Agents At Runtime	<p>When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.</p>
IP Client Capture Replay Mode	<p>The CaptureReplayMode that will be used on all ranges of the IP client.</p>
<i>Traffic Settings</i>	<i>The settings are described <a href="#">here</a>.</i>

## Traffic Settings

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

<b>Setting</b>	<b>Description</b>
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable RTP.
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	
Traffic Control Port	Set the traffic control port. Value should be in range: 1024-65535. By default, it is set to 44556.
Enable Jumbo Frame	<p>Enable this option if your test traffic requires the use of jumbo frames (Ethernet frames with more than 1500 bytes of payload).</p> <p>When you enable this option, you can then configure any of the MTU parameters in the test to any valid jumbo frame size (up to 9,000 bytes).</p>
Enable IxStack L4 Port Randomization	Select this option to enable IxStack L4 Port Randomization.
Enable UDP Port Recycling	Select this option to enable IxStack UDP Port Recycling.

Setting	Description
Enable TCP Port Recycling	Select this option to enable IxStack TCP Port Recycling.

## UDP Buffer Settings

The following table describes the UDP buffer settings.

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

## Impairment

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

Setting	Description
<i>Impairment Profiles:</i>	
	Select the <b>Add impairment profile</b> button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete impairment profile</b> 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: <b>Custom script</b> .
Script file	This parameter is available only when <b>Action Type</b> is set to <b>Custom script</b> . It allows you to add a custom script, using the <b>Upload</b> button. To remove the script, select the <b>Clear</b> button.

## Milenage

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

Setting	Description
<i>Milenage Constants</i>	
Override Milenage Constants	Enable this option to override the milenage constants.

## External Stats Server

If this option is selected, it will allow you to add an external statistic server.

The following table describes the settings required for the External Stats Server configuration.

Setting	Description
<i>External Stats Server:</i>	
Profile	This parameter allows you to upload or remove a stats server profile. Press <b>Upload</b> and load the preferred server profile, or <b>Clear</b> to dismiss one that is set.
Server Address	The address of the external stats server.

## Setting up a Profile

The External Stats Server feature allows you to forward statistic logs to an external server, thus requiring to upload a profile that defines where the stats are stored and what stats should be transferred.

**IMPORTANT** This feature is designed to support any type of external entity, but currently it supports only the Apache Kafka Plugin.

The parameters required to create the request to the external entity are configured in the **Profile** JSON file that is uploaded to Keysight Open RAN Simulators, Cloud Edition 5.1. The following structure and parameters describe the standard content of the JSON file:

Section/ Parameter	Definition	Code Sample
<i>Input section</i>	<i>Lists all the stats/config parameters used in the profile. All the parameters are already available in Keysight Open RAN Simulators, Cloud Edition 5.1. the following types are supported:</i>	
stat	It can be any stat supported in Keysight Open RAN Simulators, Cloud Edition 5.1. The stats can be filtered by any other stat from the stat response.	<p>With filter sample:</p> <pre>{     "type": "stat",     "group": "AgentStatistics",     "stat": "CPU Percent",     "name": "cpu_percent1",     "filterBy": {         "stat": "agentIP",         "value": "10.38.158.83"     } }</pre> <p>Without filter sample:</p> <pre>{     "type": "stat",     "group": "Fullcoreoverview_RegisteredAttachedUE",     "stat": "UEs Registered",     "name": "no_of_UE_Registered" }</pre>
config	It can be any parameter exposed in the UI. The path is the same as the one used by the UI to set/get a parameter (see <a href="#">Parameter sample path on the facing page</a> )	<pre>{     "type": "config",     "group": "config/nodes/ausf/ranges/1/nodeSettings",     "stat": "mcc",     "name": "mcc" }</pre>

Section/ Parameter	Definition	Code Sample
	image).	}
<i>Mappings section</i>	<i>Mapping will use any input parameter referred by name. Mapping also supports mathematical expressions to combine stats.</i>	
	<p>For example, Keysight Open RAN Simulators, Cloud Edition 5.1 exposes <code>stat1</code> and <code>stat2</code> but the user needs <code>user_stat</code> which comprises <math>(\text{stat1} + \text{stat2}) / 100</math>. The expression is evaluated and the result sent under <code>user_stat</code> name.</p>	<ul style="list-style-type: none"> <li>one parameter sample:</li> </ul> <pre>{   "type": "controlplane",   "from": "no_of_UE_Registered",   "to": "no_of_UE_Registered" }</pre> <p>OR</p> <pre>{   "type": "controlplane",   "from": "mcc",   "to": "MCC" }</pre> <ul style="list-style-type: none"> <li>with mathematical expression:</li> </ul> <pre>{   "type": "controlplane",   "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",   "to": "agent1 cpu ratio" }</pre>

### Parameter sample path

```
{
  "instanceId": "7ea3abc7-f0f6-435b-9154-125deddd101b",
  "mcc": "226",
  "mnc": "04",
  - routingIndicators: [
    1234,
    2222
  ],
  - links: [
    - {
      rel: "self",
      type: "self",
      method: "GET",
      href: "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings"
    },
    - {
      rel: "meta",
      type: "meta",
      method: "GET",
      href: "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings/$options"
    }
  ]
}
```

## Sample profile

```
{
  "profile": {
    "type": "kafka",
    "3gpp_scenario": "QUIC_ABR_DEBUG",
    "event_type": "ATTS_TOOLS_KEYSGHT_EVENT",
    "specversion": "1.1",
    "kafkatopics": "com.att.ant.stage.ATTSSKeysight.1.0",
    "kafkaschemaUrl": "https%3A%2F%2Fc1001.eastus2.uat.iebus.3pc.att.com%3A8082%2Fschemas%2Fids%2F6635&schemaId=14260",
    "kafkaHeaderBootstrapUrl": "c1001.eastus2.uat.iebus.3pc.att.com:9093",
    "kafkaHeaderSaslMechanism": "PLAIN",
    "kafkaHeaderOAuthScope": "ANT-data-feed-dev-stage",
    "kafkaUsername": "m30317@ant.att.com",
    "kafkaPassword": "August2023#",
    "input": [
      {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent1",
        "filterBy": {
          "stat": "agentIP",
          "value": "10.38.158.83"
        }
      },
      {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent2",
        "filterBy": {
          "stat": "agentIP",
          "value": "10.38.158.83"
        }
      }
    ]
  }
}
```

```

        "value":"10.38.157.97"
    }
},
{
    "type": "config",
    "group": "config/nodes/ausf/ranges/1/nodeSettings",
    "stat": "mcc",
    "name": "mcc"
},
{
    "type": "config",
    "group":
"config/nodes/ue/ranges/1/userPlane/tigerObjective/1/statelessUDP",
    "stat": "ipAddress",
    "name": "ipAddress"
},
{
    "type": "stat",
    "group": "Fullcoreoverview_RegisteredAttachedUE",
    "stat": "UEs Registered",
    "name": "no_of_UE_Registered"
},
{
    "type": "stat",
    "group": "Fullcoreoverview_PDUSessionEstablishment",
    "stat": "PDU Session Establishment Succeeded",
    "name": "no_of_PDU_Session_Established"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
    "stat": "L2-3 Device Rx Traffic",
    "name": "L3 Server::Total Bits/Sec"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
    "stat": "L2-3 Device Tx Traffic",
    "name": "L3 Client::Total Bits/Sec"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_TCPConnections",
    "stat": "TCP connections established",
    "name": "HTTP/s Handshakes Succeeded"
},
{
    "type": "stat",
    "group": "Fullcoreapplicationtraffic_TCPConnections",
    "stat": "TCP connect failed",
    "name": "HTTP/s Handshakes Failed"
}

```

```

    },
    {
      "type": "stat",
      "group": "Fullcoreapplicationtraffic_TCPConnections",
      "stat": "TCP connections closed normally",
      "name": "HTTP/s Connection Closed"
    }
  ],
  "mappings": [
    {
      "type": "controlplane",
      "from": "cpu_percent1 + cpu_percent2",
      "to": "total cpu_percent %"
    },
    {
      "type": "controlplane",
      "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",
      "to": "agent1 cpu ratio"
    },
    {
      "type": "controlplane",
      "from": "cpu_percent2/(cpu_percent1 + cpu_percent2)",
      "to": "agent2 cpu ratio"
    },
    {
      "type": "controlplane",
      "from": "mcc",
      "to": "MCC"
    },
    {
      "type": "controlplane",
      "from": "ipAddress",
      "to": "Destination IP Address"
    },
    {
      "type": "controlplane",
      "from": "no_of_UE_Registered",
      "to": "no_of_UE_Registered"
    },
    {
      "type": "controlplane",
      "from": "no_of_PDU_Session_Established",
      "to": "no_of_PDU_Session_Established"
    },
    {
      "type": "userplane",
      "from": "L3 Server::Total Bits/Sec",
      "to": "L3 Server::Total Bits/Sec"
    },
    {
      "type": "userplane",
      "from": "L3 Server::Total Bits/Sec"
    }
  ]
}

```

```

        "from": "L3 Client::Total Bits/Sec",
        "to": "L3 Client::Total Bits/Sec"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Handshakes Succeeded",
        "to": "HTTP/s Handshakes Succeeded"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Handshakes Failed",
        "to": "HTTP/s Handshakes Failed"
    },
    {
        "type": "userplane",
        "from": "HTTP/s Connection Closed",
        "to": "HTTP/s Connection Closed"
    }
]
}
}

```

**Event body sent to Kafka**

```

[
{
    "eventBody": {
        "id": "wireless-0acbc45b-8777-4250-a3ec-4f00e47399c8_39",
        "time": "2024-02-29T13:57:35Z",
        "type": "ATTS-TOOLS-KEYSIGHT-EVENT",
        "specversion": "1.1",
        "source": "https://10.38.157.61/wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
        "datacontenttype": "application/json",
        "payload": [
            {
                "type": "resource_info",
                "resource_info": {
                    "simulated_tool_info": [
                        {
                            "tool_name": "LoadCore",
                            "middleware_ip": "10.38.157.61"
                        }
                    ],
                    "network_type": "5G",
                    "3gpp_scenario": "QUIC_ABR_DEBUG"
                }
            },
            {
                "type": "test_execution_result",
            }
        ]
    }
}
]

```

```

    "test_execution_result": {
        "control_plane_result": {
            "Destination IP Address": "20.0.6.10",
            "MCC": "226",
            "agent1 cpu ratio": "0.455321",
            "agent2 cpu ratio": "0.544679",
            "no_of_PDU_Session_Established": "100",
            "no_of_UE_Registered": "0",
            "total cpu_percent %": "3.0902"
        },
        "userplane_plane_result": {
            "L3 Client::Total Bits/Sec": "0",
            "L3 Server::Total Bits/Sec": "0"
        }
    },
    {
        "type": "test_execution_details",
        "test_execution_details": {
            "testName": "4 - Full Core Base Config",
            "testSessionID": "wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
            "UserID": "admin@example.org",
            "testStatus": "STOPPING",
            "testStartTime": "2024-02-29T13:55:40Z",
            "testDuration": 105,
            "testStopTime": "2024-02-29T13:57:31Z"
        }
    }
],
},
"payloadType": "JSON",
"value": {}
}
]

```

## Global Playlists

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

Setting	Description
<i>Global Playlists:</i>	
	Select the <b>Add Global Playlist</b> button to add a new playlist to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete Global Playlist</b> button to remove the playlist from your test configuration.

Setting	Description
Name	Each playlist profile is uniquely identified by a name. You can accept the value provided by LoadCore or overwrite it with your own value.
Playlist file (.csv)	It allows you to add a custom playlist, using the <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.

# IP Client configuration settings



The IP Client configuration settings are described in the topics listed below.

## Topics:

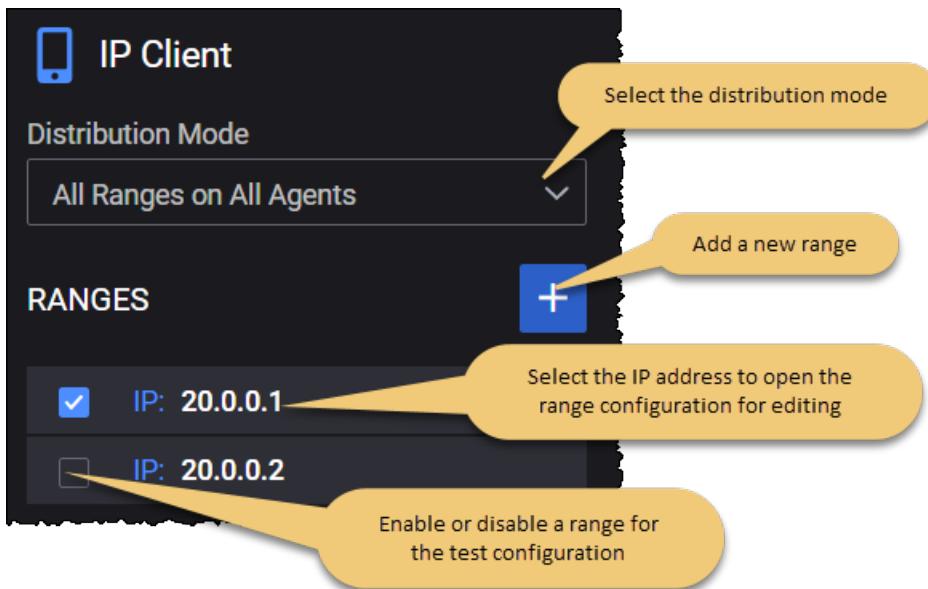
<b>IP Client Ranges panel</b>	922
<b>IP Client Range panel</b>	923
<b>IP Client interface settings</b>	924
<b>IP Client Timeline</b>	925
<b>IP Client User Plane</b>	925
Stateless UDP Traffic	926
Data Traffic	927
Voice Traffic	931
Video OTT Traffic	946
DNS Client Traffic	950
ICMP Client	953
Capture Replay	954
Synthetic	955
UDG	957
REST API Client	961

## IP Client Ranges panel

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

- Set the **Distribution Mode**:
  - **All Ranges on All Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UPF node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1 and agent2, range2 on agent1 and agent2, range 3 on agent1 and agent2.
  - **Round Robin Ranges on Agents** - influences the way configuration is distributed in case of multiple agents assigned on the UPF node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1, range2 on agent2, range3 on agent1.
- Add a new IP Client range to your test configuration.
- Open a IP Client range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

For example ...



## IP Client Range panel

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

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

## IP Client range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
	Select the <b>Create Range Copies</b> button to create copies of your range. Also, you can specify the number of ranges to be created.
Device Under Test	Enable this option if your IP Client is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the IP Client functionality

<b>Setting</b>	<b>Description</b>
	(if it is selected in the Topology window).
Range Count	The number of IP clients in the IP Client range.
Remote Server	The IP address of the remote server.
<i>Range Settings:</i>	
Interface Settings	Each IP Client range requires the configuration of the interface settings, through which an IP Client instance enables connectivity and interaction with other functions in the network. These settings are described in <a href="#">IP Client interface settings</a> .
Timeline	These settings are described <a href="#">IP Client Timeline</a> .
User Plane	These settings are described in <a href="#">IP Client User Plane</a> .

## IP Client interface settings

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

<b>Connectivity Settings</b>	<b>Description</b>
<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.
IP Address Increment	The value by which the IP addresses will be incremented.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	The Maximum Transmission Unit (MTU) for this range. MTU specifies the largest packet that an Ethernet frame can carry.
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>MAC</i>	Select the MAC address to open the MAC configuration panel for editing
MAC Address	Hardware MAC address.

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

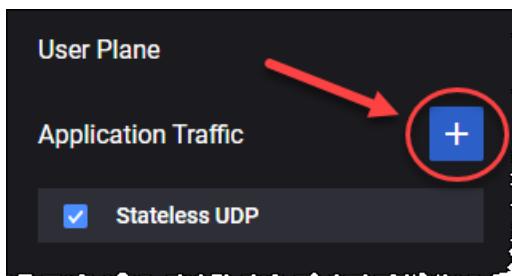
## IP Client Timeline

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

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

## IP Client User Plane

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



Parameter	Description
	Select this button to add a new application traffic objective. The objective can be: <ul style="list-style-type: none"> <li><b>Stateless UDP</b></li> <li><b>Data</b></li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>Voice</b></li> <li>• <b>Video OTT</b></li> <li>• <b>DNS Client</b></li> <li>• <b>ICMP Client</b></li> <li>• <b>Capture Replay</b></li> <li>• <b>Synthetic</b></li> <li>• <b>UDG</b></li> </ul>
	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 <a href="#">Stateless UDP Traffic</a> .
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">Data Traffic</a> .
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">Voice Traffic</a> .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">Video OTT Traffic</a> .
DNS Client	For the settings required to configure the DNS Client objective, refer to <a href="#">DNS Client Traffic</a> .
ICMP Client	For the settings required to configure the ICMP Client objective, refer to <a href="#">ICMP Client Traffic</a> .
Capture Relay	For the settings required to configure the Capture Replay objective, refer to <a href="#">Capture Replay</a> .
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to <a href="#">Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG traffic objective, refer to <a href="#">UDG Traffic</a> .
REST API Client	For the settings required to configure the REST API Client objective, refer to <a href="#">REST API Client</a> .

## Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Stateless UDP</b> .
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 <b>uplink</b> and can not be modified.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Payload Size	The size of the packet payload, in bytes.
Delay (s)	The time to wait before the application traffic flows start.
Destination UDP Port	The start destination port number to place in the UDP header.
Source UDP Port	The source port number to place in the UDP header.

## Data Traffic

The following table describes the Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Data</b> .
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 <b>Throughput</b> . The other options are: <b>Concurrent Connections</b> and <b>Connections Rate</b> .
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connections Rate per Second	Set the value for connections rate per second. This parameter is available only when Objective type is set to <b>Connections Rate</b> .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be

Parameter	Description
	generated.
Optimize Throughput (per IP Client)	Select this option to enable it.
Connection Multiplier (per IP Client)	Set the connection multiplier value.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
MSS	<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 IP Session has been established.
TCP Settings	<i>Select the pane to open the TCP settings.</i>
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.

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

## Flow

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

Parameter	Description
	Click the <b>Delete Flow</b> 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"> <li>If <a href="#">Optimize Throughput (per IP Client)</a> option is enabled: <b>TCP</b>, <b>TLS</b>, <b>QUIC</b> or <b>UDP</b>.</li> <li>If <a href="#">Optimize Throughput (per IP Client)</a> option is disabled: <b>TCP</b>, <b>TLS</b> or <b>UDP</b>.</li> </ul>
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get</b>, <b>HTTP Put</b>, <b>HTTP Post</b> and <b>FTP</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get</b>, <b>HTTPS Put</b> and <b>HTTPS Post</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Get</b>, <b>HTTP3 Put</b> and <b>HTTP3 Post</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional</b> (a flow in which a UDP client communicates with a server over a bidirectional datagram socket).</li> </ul>
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.

Parameter	Description
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.
Tx Packets Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
RX Packets Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
URL	The URL that is being accessed by the flow's protocol.
Max Transactions per Connection	Set the value for this parameter.
Enable DNS Query Per Connection	Select the check-box to process only one DNS query per TCP connection.

## Custom Parameters

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

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

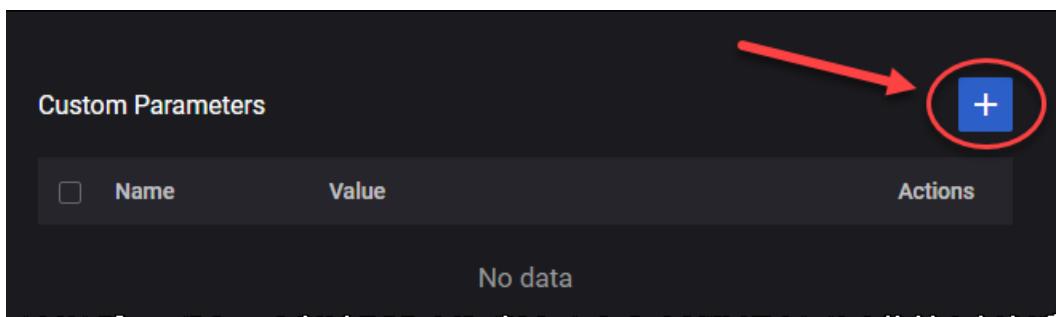
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

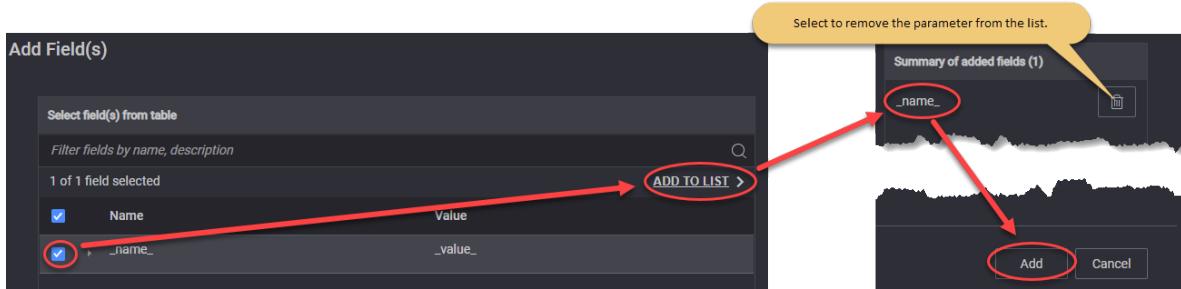
2. Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



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

## Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Voice</b> .
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 <b>Simulated Users</b> and cannot be changed.
Ramp Up Rate	Set the value for this parameter.
Ramp Down Rate	Set the value for this parameter.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.
Call Type	<p>Select the type of call from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>Basic Call</b></li> <li>• <b>Basic Call Mo</b> (Mobile Originated)</li> <li>• <b>Basic Call Mt</b> (Mobile Terminated)</li> <li>• <b>Custom Flow</b></li> </ul> <p>When creating a new test or when adding a new UE range, the Call Type default option is the <b>Basic Call</b>, which allows you to run a basic SIP call without the IMS entity and with DN simulating the Mobile Terminating (MT) side.</p>

Parameter	Description
	When selecting <b>Basic Call MO/Basic Call MT</b> , the app will use a predefined SIP Flow intended for the use-case in which a DUT IMS or simulated IMS is involved. If the test requirements need an extended set of SIP flows or higher level of flexibility, it is recommended to use the <b>Custom Flow</b> Call Type, which enables the Flow Editor.
Flow Editor:	<p><b>IMPORTANT</b> This configurator becomes available only if Call Type is set to Custom Flow.</p> <p>Click to open the page and create a particular state machine for SIP calls that allows you a higher flexibility to customize the SIP message sequence and SIP headers/SDP body as desired. For settings, refer to <a href="#">Flow Editor</a> section.</p>
Dial Plan:	<i>For the settings required to configure the dial plan, refer to <a href="#">Dial Plan</a>.</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"> <li>• <b>TCP</b> - Transmission Control Protocol</li> <li>• <b>TLS</b> - Transport Layer Security</li> <li>• <b>UDP</b> - User Datagram Protocol</li> </ul>
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	<i>For more details about these settings, refer to <a href="#">Advanced SIP Settings</a>.</i>
<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.
Audio settings:	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
Video Settings:	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>

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

## Flow Editor

Press  to open the editor's window. The following settings are available:

Parameter	Description
Procedures Library	<p><b>TIP</b> This library can also be accessed from Test Overview &gt; Procedures Library, while the procedures are managed from the <a href="#">Settings &gt; Resource Library</a>.</p> <p>Select to access the Procedures Library, where you will find the following categories:</p> <ul style="list-style-type: none"> <li>• <b>SIP</b> - will include the procedures related to SIP signaling.</li> <li>• <b>Media</b> - will include the procedures related to media (audio or/and video)</li> <li>• <b>Flow</b> - will include the Start and Stop procedures used to define an iteration. The number of iterations can be configured per each UE range on the Voice objective, Dial Plan section (0 meaning infinite loops).</li> </ul> <p>See <a href="#">Procedures Library</a> for more information.</p>
Current Range	This field will be automatically populated with the name of the UE range on which the Voice application traffic is configured.
Add required	Add the procedures required for this custom flow.

Parameter	Description
procedures first > Procedures	
Linked Range	Select from the drop-down the UE range that will be connected. Then, add the procedures corresponding to the configuration of state machine.

Note that every procedure added under the Procedures list includes an **Add +** button and an **Expand** button:

- Use the Expand button to see the **Next On Success** and **Next on Error** configuration fields for the respective procedure. Proceed on setting up these fields for each procedure added.
- Use the **Add** button to add more steps to the procedure. Set the procedures as above.
- The red connections that appear between procedures will let you know how these are connected.

See also the [Procedures Resources \(SIP/Media/Flow\)](#) section for complete information on:

- [procedures resources and their management](#)
- [adding predefined procedures](#) from the Resource Library
- [using the Flow Editor](#) and other configurations required
- [creating a procedure from scratch](#)

## Dial Plan

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

Parameter	Description
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).
MCC	Set the Mobile Country Code (MCC) value.
MNC	Set the Mobile Network Code (MNC) value.
MSIN	Set the MSIN value. The Mobile Subscriber Identification Number (MSIN) is a number that a wireless operator uses to uniquely identify a mobile phone. It is—at most—10-digits long. The MSIN is used (in combination with the MCC and MNC) to form the International Mobile Subscriber Identity (IMSI) number.
IMSI Phone Increment	The value by which the IMSI phone number is incremented.
Destination Phone	The destination phone number.
Destination Phone	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 Port	The destination port number.

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
<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"> <li>• <b>AMR</b> - 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.</li> <li>• <b>AMR-WB</b> - 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.</li> <li>• <b>EVS</b> - 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.</li> <li>• <b>PCMU</b></li> <li>• <b>PCMA</b></li> <li>• <b>iLBC</b></li> <li>• <b>G722</b></li> <li>• <b>G723</b></li> </ul>

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

**AMR/AMR-WB**

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth efficient:</b> In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added.</li> <li>• <b>Octet aligned:</b> 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.</li> </ul>
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"> <li>• <b>Full header</b> - 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.</li> <li>• <b>Compact</b> - 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.</li> </ul>

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.

### Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
Video Codecs	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

### MSRP Settings

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

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

## Advanced SIP Settings

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

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

### SIP Custom Headers

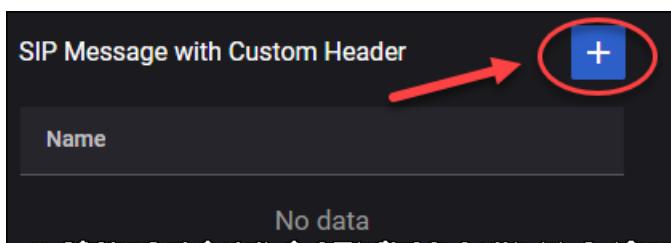
From the SIP Message with Custom Header pane, select the **Add** button to add a new SIP message.

**NOTE**

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

For each message, you can:

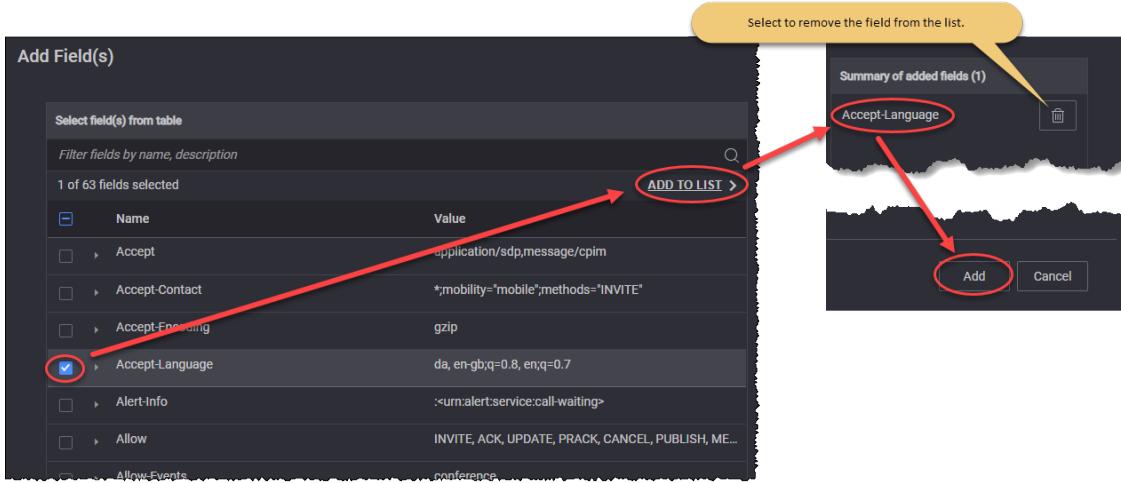
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
  - Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



The following custom header are available:

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

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
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

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
	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

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
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.

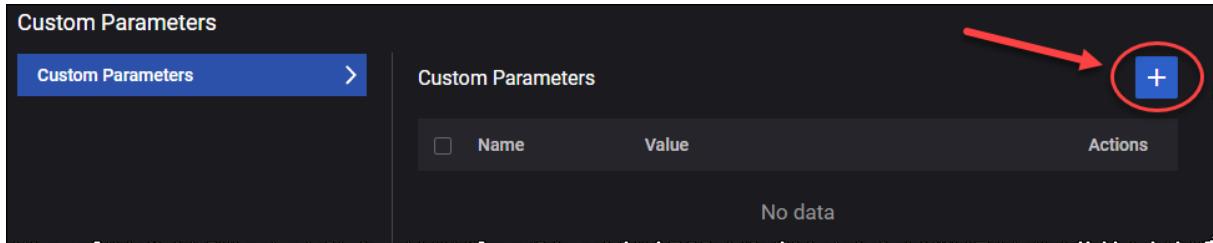
Parameter	Description
Username	Provide the username.
Password	Provide the password.
Authentication Type	Select the authentication type: <ul style="list-style-type: none"> <li>• <b>Digest MD5</b></li> <li>• <b>AKAv1</b></li> <li>• <b>AKAv2</b></li> <li>• <b>ProxyDefined</b></li> </ul>

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

## Custom Parameters

You can add custom parameters as follows:

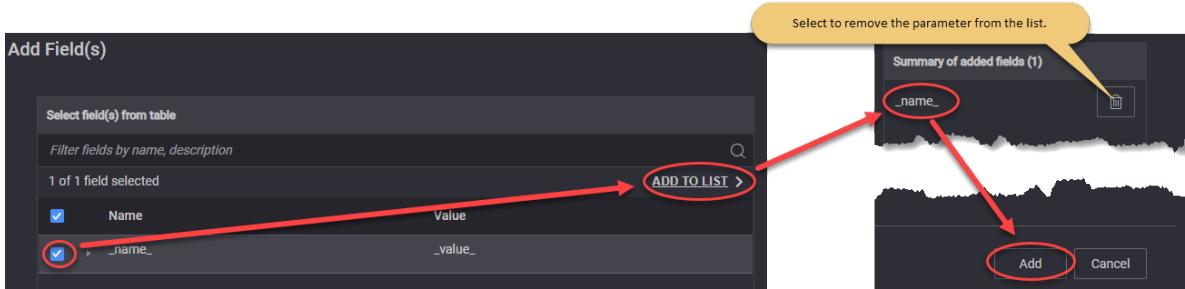
1. The Custom Parameters panel, select the **Add** button.



The Add Field(s) opens.

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

### For example ...



The following custom parameters are available:

Parameter	Description	Value
DelayBefore SIPInvite	Delay in 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
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 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"> <li>• <b>hmac-sha-1-96</b></li> <li>• <b>aes-gmac</b></li> <li>• <b>null</b></li> </ul>
Encryption Algorithm	Select the encryption algorithm: <ul style="list-style-type: none"> <li>• <b>aes-gcm</b></li> <li>• <b>aes-cbc</b></li> <li>• <b>null</b></li> </ul>

## 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 <b>Video OTT</b> .
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: <b>Simulated Users</b> or <b>Throughput</b> .
Ramp Up Rate	Set the value for this parameter.
Ramp Down Rate	Set the value for this parameter.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.  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 IP Session has been established.

Parameter	Description
Advanced OTT	Select the <b>Open Advanced OTT</b> button to enable and configure <a href="#">Advanced OTT Settings</a> .

## 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"> <li>To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul>
<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"> <li><b>DASH</b></li> <li><b>HLS</b></li> </ul>
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
URL	Select the URL from the drop-down list populated with the defined on the server.
Play Until End	If this option is enabled, the Play Duration field is disabled and the original playtime is used.
Transport	Select the transport protocol from the drop-down list. Available options: <ul style="list-style-type: none"> <li><b>HTTP</b></li> <li><b>HTTPS</b></li> <li><b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Quality Control</a> pane.

Parameter	Description
Advanced Client settings	These settings are presented in the <a href="#">Advanced Client Settings</a> 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: <b>Disabled</b> or <b>Mode 0</b> .
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Adaptive Bit Rate</b></li> <li>• <b>Quality Predefined Levels</b></li> <li>• <b>Lowest Quality</b></li> <li>• <b>Highest Quality</b></li> </ul>
Number of segments	This field is available and editable only when the Quality Control Mode is set to <b>Adaptive Bit Rate</b> .
<i>Play Profiles:</i> The following settings are available and editable only when the Quality Control Mode is set to <b>Quality Predefined Levels</b> .	
	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"> <li>• <b>Stay at Current Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lower Bitrate</b></li> <li>• <b>Change to the Higher Bitrate</b></li> </ul>

Parameter	Description
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to <b>Change to Higher Bitrate</b> or <b>Change to Lower Bitrate</b> .
Play Until End	If this check box is selected, the <b>Play duration</b> field is disabled and the original playtime is used.
Play duration(sec)	This field is available only if the <b>Play Until End</b> check box is not selected. It allows you to set a custom playtime.

## Advanced Client Settings

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

Parameter	Description
Timeshift for Live	Set a value for this field. 0 means no timeshift.
Enable DNS Query Per Connection	Select the check box to process only one DNS query per TCP connection.
Custom Parameters	For more details, refer to <a href="#">Custom Parameters and Custom Headers</a> .
Custom Headers	For more details, refer to <a href="#">Custom Parameters and Custom Headers</a> .

## Custom Parameters and Custom Headers

You can add custom parameters or custom header fields by selecting the required pane:

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

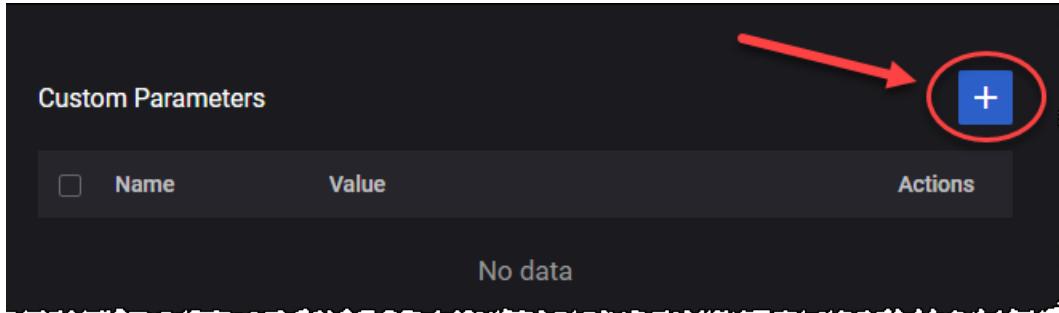
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

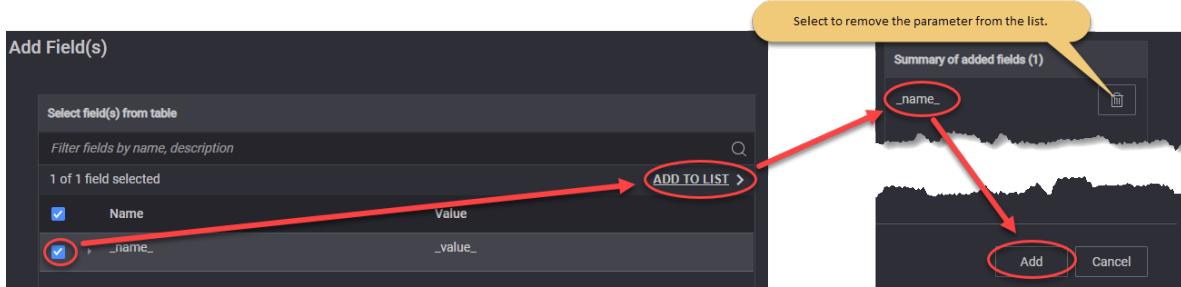
2. Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



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

## DNS Client Traffic

The following table describes the DNS Client Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>DNS Client</b> .
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 <b>Simulated Users</b> and cannot be changed.
Connection multiplier (per IP Client)	Set the value for the connection multiplier.
Ramp Up Rate	Set the value for this parameter.
Ramp Down	Set the value for this parameter.

Parameter	Description
Rate	
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 IP Session has been established.
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"> <li>• To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>• To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul> <p>Refer to <a href="#">Flow</a> for a description of the configuration settings for these traffic flows.</p> <p>Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Flow</b> button to remove the flow from your configuration.
Type	By default, the type is set to <b>DNS Client</b> .
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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.

## Custom Parameters

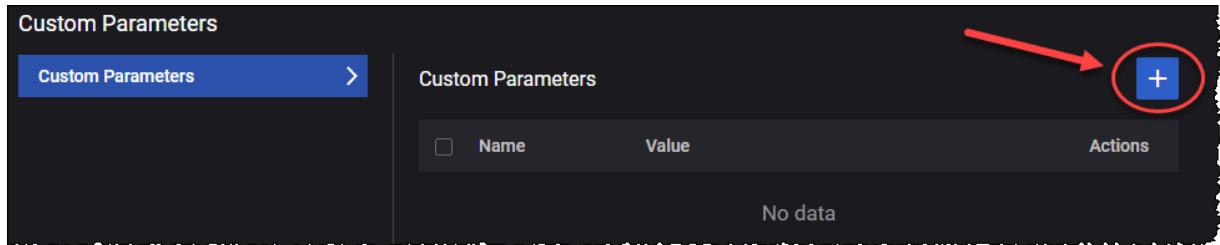
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

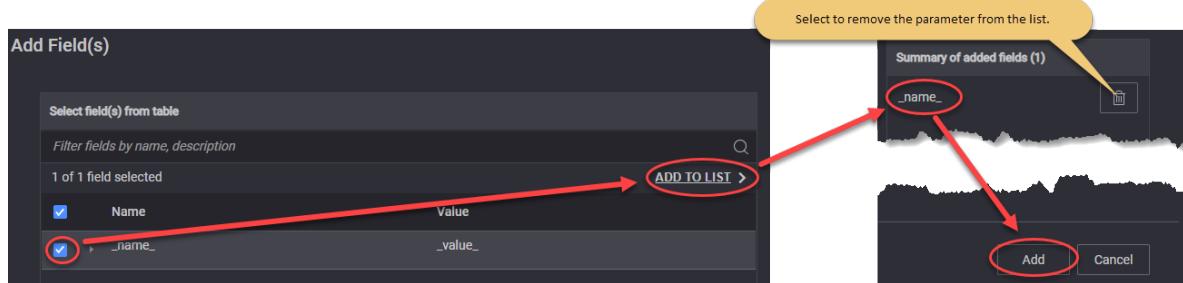
2. Select the **Add** button.



The Add Field(s) opens.

- 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 <b>ICMP Client</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each IP Session has been established.
Objective Type	By default, this parameter is set to <b>Simulated Users</b> and cannot be changed.
Traffic Flow	Refer to <a href="#">Traffic Flow</a> for a description of the configuration settings for these traffic flows.

## Traffic Flow

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

Parameter	Description
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). Iterations is the number of times you want this flow of actions to be executed.
Interval (ms)	Set the interval value.
Timeout (ms)	Set the timeout value.

## Capture Replay

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>Capture Replay</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Ramp Up Rate	Set the value for the this parameter.
Ramp Down Rate	Set the value for the this parameter.
Capture File	It allows you to upload a capture file, using the <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b> (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (option enabled).
Start Delay (s)	The number of seconds to wait after all IPs have been configured.

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: <b>Initiator</b> and <b>Responder</b> . Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> (option disabled).

## Synthetic

The following table describes the Synthetic parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>Synthetic</b> .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be 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: <b>IPv4</b> or <b>IPv6</b> .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an

Parameter	Description
	acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).
Selective Acknowledgments	If necessary, enable this option.
<i>UDP Settings</i>	
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the UDP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the UDP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min source port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max source port	The Max value specifies the upper bound (the highest permissible port number).

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

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Client Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
Server Burst Interval	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
Server Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

## UDG

The following table describes the UDG parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>UDG</b> .
Label	Set the label name. You can accept the value provided by CoreSIM or overwrite it with your own value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that

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

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

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

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>UDP</b> .
Out of Band Signaling	<p>Select this check-box to enable OOB signaling. More details about the required parameters <a href="#">here</a>.</p> <p><b>IMPORTANT</b> To use the OOB feature, the OOB interface must be set in Agent Management window.</p>
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Reconnect Timeout (ms)	The time interval after which the client attempts to reconnect after the connection was interrupted. 0 means that reconnect is disabled.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

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

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

Parameter	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.
Remote Address	The remote IP address.
Port	Set the used port.

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

Parameter	Description
UGD Test Type	Select the test type from the drop-down list. Available options: <b>Transmission</b> or <b>Ping-pong</b> . For each test type, the parameters are described below.
<i>Transmission</i>	
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Server Burst Interval	The time interval at which the server sends packet bursts.
Server Burst Interval Unit	Select the server burst interval unit. Available options: <b>Millisecond</b> or <b>Microsecond</b> .
Server Burst Size (packets)	The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
<i>Ping-pong</i>	
Ping Direction	Set the ping direction. Available options: <b>Upstream</b> or <b>Downstream</b> .
Ping Interval	Set the ping time interval.
Ping Interval Unit	Set the ping interval unit. Available options: <b>Millisecond</b> or <b>Microsecond</b> .
Pong Number	Set the value for the pong number.

Parameter	Description
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.

## REST API Client

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

The following table describes the REST API Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>REST API Client</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	This field is set to <b>Simulated Users</b> and cannot be modified.
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>TLS</b> .
REST API Flow	<p>The name of list of REST API Client sequential operations and transitions emulated by each REST API Client.</p> <p>The REST API Flow is initially loaded into LoadCore's Resource Library, and then added to the test as a <a href="#">Global Playlists</a>. The list is defined in CSV format, following specific rules. Refer to <a href="#">Work with the Resource Library on page 73</a> section for further information.</p>
Ramp Up Rate	Set the value for the Activation UE rate.
Ramp Down Rate	Set the value for the Deactivation UE rate.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before starting the Attacks objective traffic.
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .
Iterations	If is set to <b>0</b> , it will be iterated on continuous loop during sustain time. If set to <b>1</b> , it will be executed only one time. <b>IMPORTANT</b> Values greater than 1 are not allowed.
Max Transactions per Connection	The maximum amount of transactions an application can make on one connection.

Parameter	Description
Enable DNS Query per Connection	If enabled, will process only one DNS query per TCP connection.
DNN	Select the DNN value for the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.  The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Selective Acknowledgments	Select the toggle button to enable this option.
<i>TLS Settings</i>	See <a href="#">TLS Settings</a> table for more details.

Parameter	Description
Custom Parameters	For more details, refer to <a href="#">Custom parameters</a> .

## TLS Settings

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

## Custom Parameters

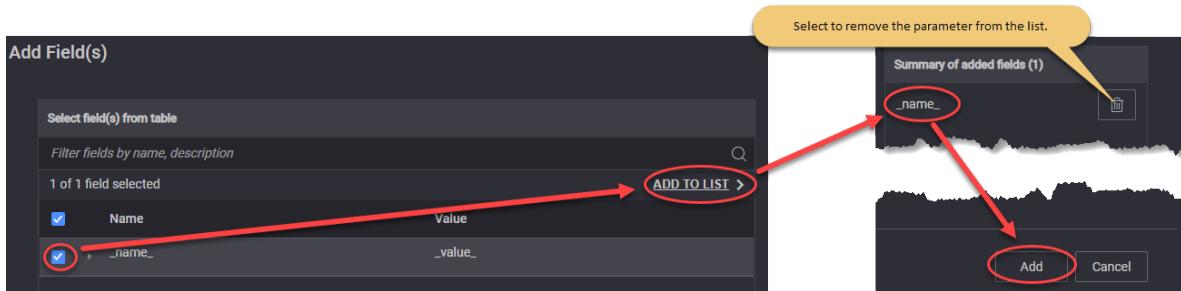
From this section you can add custom parameters fields:

- **Custom Parameters**

You can add custom parameters as follows:

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

**For example ...**



## How to Configure the REST API Client

1. Define your REST API flow in an CSV file, following the rules described in the [REST Client Flow specifications](#).
2. Load the CSV as a Global Playlist in LoadCore user interface:
  - a. Go to **Global Settings > Global Playlist**.
  - b. Add a new Playlist using the **+** button.
  - c. **Name** the new Playlist - it will be used in the REST API Client application configuration.
  - d. **Upload** the CSV created at **Step 1**.
3. In the User Plane UE section, select the **REST API Client** application traffic.
4. Set all necessary parameters on required by the application (see [REST API parameters table](#) above):
  - on **Transport protocol** select **TCP** or **TLS** (version 1.2 and 1.3 configurable from TLS Settings).
  - the **Objective type** is automatically set to **Simulated users**.
  - add the **REST API Flow** name that defines the REST sequence of actions defined in the Global Playlist.
  - set the **Max Transactions per Connection**- for REST API Client application, one "Transaction" points to all REST actions (HTTP requests) specified in REST flow.
  - Set all other common parameters.

## REST Client Flow specifications

The REST Client flow will be specified in CSV format state-by-state. For each State in flow, three main commands must be specified, and one special command at the end of list:

Command	Condition	Description
<b>Action</b>	Mandatory	<p>Indicates what actions should be executed in the current State and what transitions can be executed. The following rules are in place:</p> <ul style="list-style-type: none"> <li>• up to 4 transitions are allowed. Maximum 4 pairs of (Conditions, NextState) are used from CSV.</li> <li>• Method, Headers and Body should be specified in separate columns.</li> <li>• Method, Headers and Body can contain dynamic parts specified by flow user variables.</li> </ul>
<b>Extract</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>Specifies if some elements from the last HTTP response should be extracted in user variables for further utilization in flow:</p> <ul style="list-style-type: none"> <li>• extractions are specified using (backqoute_separated_path, userVar) pairs.</li> <li>• up to 3 extractions per REST(HTTP) response are allowed.</li> </ul>
<b>Statistics</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>User-defined Counters can be incremented when the condition is fulfilled. The configuration is done in pairs of (condition, UserCounter).</p>
<b>ENDMARKER</b>	Mandatory	This special command is mandatory to indicate the end of REST API flow. No other command will be executed after the ENDMARKER was executed. It can be inserted anywhere in the Playlist, on the first column.

## REST user flow variables

There are 10 flow variables with predefined names (userVar1, userVar2,...,userVar10) available for store extracted values from REST Commands during flow duration. On each REST Command, you can configure what to extract from the received Response, and in what variable.

Each variable can be overwritten at anytime, therefore a variable can be persistent during the flow duration, or only temporary, until overwrite.

# Triple Play Server configuration settings

In LoadCore, the Triple Play Server has three important components:

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

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

## Topics:

<b>CSCF Range panel</b>	<b>966</b>
<b>Media Function Range panel</b>	<b>967</b>
<b>Data/Video configuration settings</b>	<b>968</b>
Data/Video Ranges panel	969
Data/Video Range panel	969
Data/Video interface settings	970
Data/Video User Plane	971
Data/Video Throttling settings	998

## CSCF Range panel

When you select the 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. Also, you can designate the range as a **Device Under Test**.

### CSCF range controls and settings

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

Setting	Description
Device Under Test	Enable this option if your CSCF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the CSCF functionality (if it is selected in the Topology window).
<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.
Force IPsec Null Encryption	If enabled, it forces IPsec null encryption, therefore not encrypting the ESP traffic.

Setting	Description
<i>Authentication Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: <b>keysight.com</b> .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: <b>Digest</b> , <b>AKAv2</b> or <b>AKAv1</b> .
Algorithm	Select the algorithm from the drop-down list. Available options: <b>MD5</b> , <b>MD5-Sess</b> , <b>SHA256</b> or <b>SHA256-Sess</b> .
Quality of Protection	Select an option from the drop-down list: <b>auth</b> or <b>auth-init</b> .
<i>Interface Settings</i>	
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).
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

## Media Function Range panel

When you select the 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>	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).
<i>MAC</i>	Select the MAC address to open the MAC configuration panel for editing.
MAC Address	MAC Address Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
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><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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.

## Data/Video configuration settings

The Data/Video configuration settings are described in the topics listed below.

### Topics:

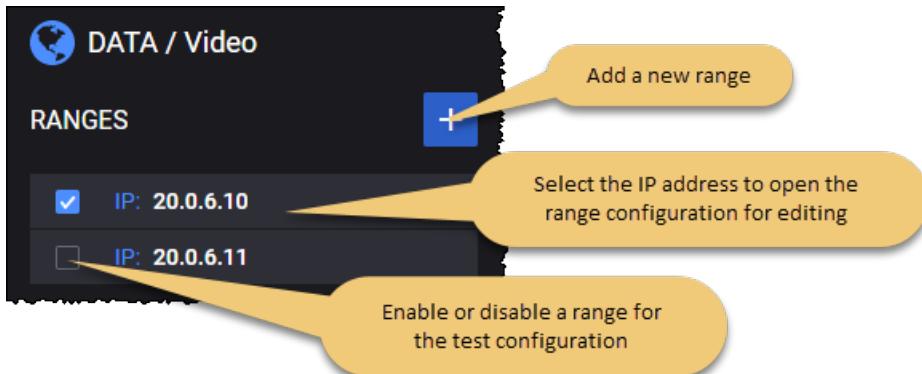
<b>Data/Video Ranges panel</b> .....	<b>969</b>
<b>Data/Video Range panel</b> .....	<b>969</b>
<b>Data/Video interface settings</b> .....	<b>970</b>
<b>Data/Video User Plane</b> .....	<b>971</b>
<b>Data/Video Throttling settings</b> .....	<b>998</b>

## Data/Video Ranges panel

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

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

**For example ...**



## Data/Video Range panel

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

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

## Data/Video range controls and settings

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

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

Setting	Description
<i>Range:</i>	
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
	Select the <b>Create Range Copies</b> button to create copies of your range. Also, you can specify the number of ranges to be created.

Setting	Description
Device Under Test	Enable this option if your Data/Video is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the Data/Video functionality (if it is selected in the Topology window).
Range Count	Set the value for the range count.
<i>Range Settings:</i>	
Interface Settings	These settings are described in <a href="#">Data/Video interface settings</a> .
User Plane	These settings are described in <a href="#">Data/Video User Plane</a> .
Throttling Settings	These settings are described in <a href="#">Data/Video Throttling settings</a> .

## Data/Video interface settings

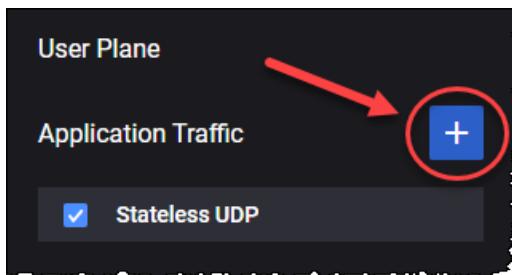
The following table describes the **Connectivity Settings** that you configure for each Data/Video range.

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

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><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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.

## Data/Video User Plane

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



Parameter	Description
	<p>Select this button to add a new application traffic objective. The objective can be:</p> <ul style="list-style-type: none"> <li>• <b>Stateless UDP</b></li> <li>• <b>Data</b></li> <li>• <b>Voice</b></li> <li>• <b>Video OTT</b></li> <li>• <b>DNS Server</b></li> <li>• <b>Capture Replay</b></li> <li>• Synthetic</li> <li>• UDG</li> </ul>
	Select this button to remove the application traffic objective from your test configuration.

Parameter	Description
Stateless UDP	For the settings required to configure the Stateless UDP traffic objective, refer to <a href="#">Stateless UDP Traffic</a> .
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">Data Traffic</a> .
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">Voice Traffic</a> .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">Video OTT Traffic</a> .
DNS Server	For the settings required to configure the DNS Server objective, refer to <a href="#">DNS Server Traffic</a> .
Capture Relay	For the settings required to configure the Capture Replay objective, refer to <a href="#">Capture Replay</a> .
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to <a href="#">Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG traffic objective, refer to <a href="#">UDG Traffic</a> .

## Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Stateless UDP</b> .
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 <b>downlink</b> and can not be modified since on the Data/Video you can only configure the downlink flow.
Packet Rate	The rate at which the test generates downlink packets, measured in packets per second (pps).
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Payload Size	The size of the packet payload, in bytes.
Destination UDP Port Start	The start destination port number to place in the UDP header.

Parameter	Description
Destination UDP Port Count	Total number of UDP ports in this range.
Source UDP Port	The source port number to place in the UDP header.

## Data Traffic

The following table describes the DN Data Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Data</b> .
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>
TCP Settings	<i>Select the pane to open the TCP settings.</i>
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
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.

<b>Parameter</b>	<b>Description</b>
Selective Acknowledgments	Select the toggle button to enable this option.
<i>Application Servers</i>	<p><i>Each Application Traffic entry requires an application server definition, and can support multiple such definitions.</i></p> <ul style="list-style-type: none"><li>• <i>To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.</i></li><li>• <i>To add another application server, click the <b>Add Server</b> button. LoadCore will open the Server panel where you will select the server type and configure the server settings.</i></li></ul> <p><i>Refer to <a href="#">Server</a> (below) for a description of the configuration settings required by the application server.</i></p> <p><i>Also, you can add <a href="#">custom parameters</a>, based on your test configuration requirements.</i></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 <b>Delete Server</b> 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: <b>TCP</b> , <b>TLS</b> , <b>QUIC</b> or <b>UDP</b> .
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"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get Responder</b>, <b>HTTP Put Responder</b>, <b>HTTP Post Responder</b>, <b>HTTP Server</b> and <b>FTP Responder</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get Responder</b>, <b>HTTPS Put Responder</b>, <b>HTTPS Post Responder</b> and <b>HTTPS Server</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Server</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional Responder</b>.</li> </ul>
Port	The port used by the application server.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.

## Custom Parameters

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

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

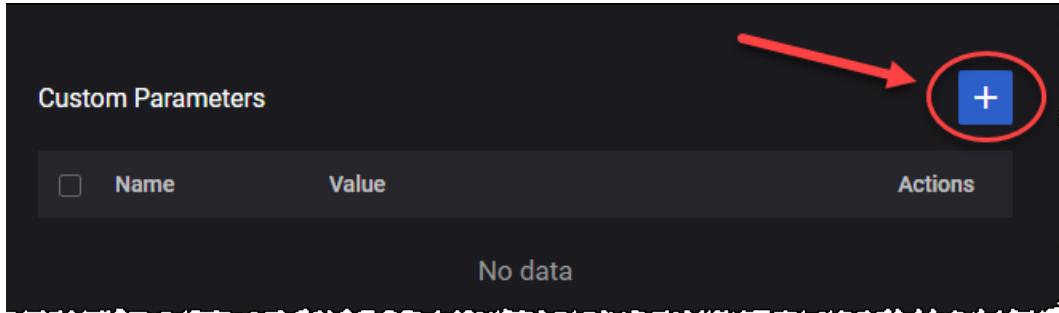
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

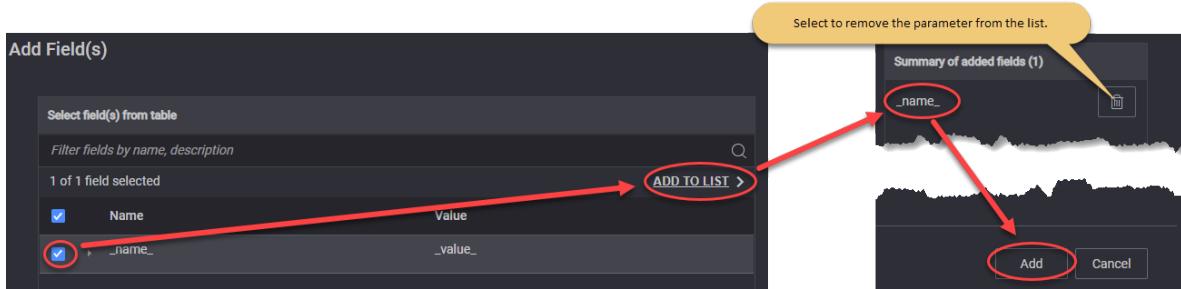
2. Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



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

## Voice Traffic

The following table describes the Voice Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Voice</b> .
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 <b>Simulated Users</b> 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.

Parameter	Description
Dial Plan:	<i>For the settings required to configure the dial plan, refer to <a href="#">Dial Plan</a>.</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"> <li>• <b>TCP</b> - Transmission Control Protocol</li> <li>• <b>TLS</b> - Transport Layer Security</li> <li>• <b>UDP</b> - User Datagram Protocol</li> </ul>
Domain	Provide the domain name.
Enable IPSEC	Select this option to enable IPSEC.
Advanced SIP Settings	<i>For more details about these settings, refer to <a href="#">Advanced SIP Settings</a>.</i>
<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.
Audio settings:	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
Video Settings:	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
MSRP Settings:	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
Advanced Media Settings:	
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	Select the template from the drop-down list:

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

## Dial Plan

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

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

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
<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"> <li>• <b>AMR</b> - 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.</li> <li>• <b>AMR-WB</b> - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data</li> </ul>

Parameter	Description
	<p>compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP.</p> <ul style="list-style-type: none"> <li>• <b>EVS</b> - 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.</li> <li>• <a href="#"><b>PCMU</b></a></li> <li>• <a href="#"><b>PCMA</b></a></li> <li>• <a href="#"><b>iLBC</b></a></li> <li>• <a href="#"><b>G722</b></a></li> <li>• <a href="#"><b>G723</b></a></li> <li>• <a href="#"><b>G729</b></a></li> </ul> <p>The parameters of each audio codec are presented below.</p>

## AMR/AMR-WB

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

## EVS

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet.
Payload Type	Specifies the audio payload type.
Payload Format	The following options are available: <ul style="list-style-type: none"> <li><b>Full header</b> - 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.</li> <li><b>Compact</b> - 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.</li> </ul>
Bitrate	Indicates the mode(bitrate) of the EVS codec. Select the value from the drop-down list.

### PCMU/PCMA/iLBC/G722/G723/G729

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

### Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
Video Codecs	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

## MSRP Settings

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

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

## Advanced SIP Settings

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

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

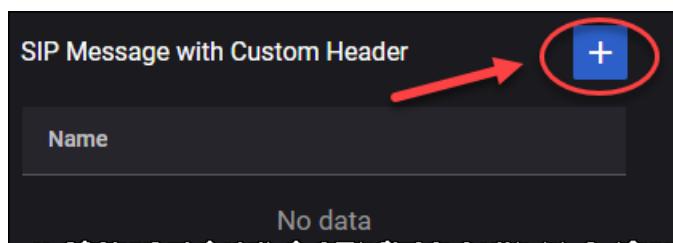
### SIP Custom Headers

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

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

For each message, you can:

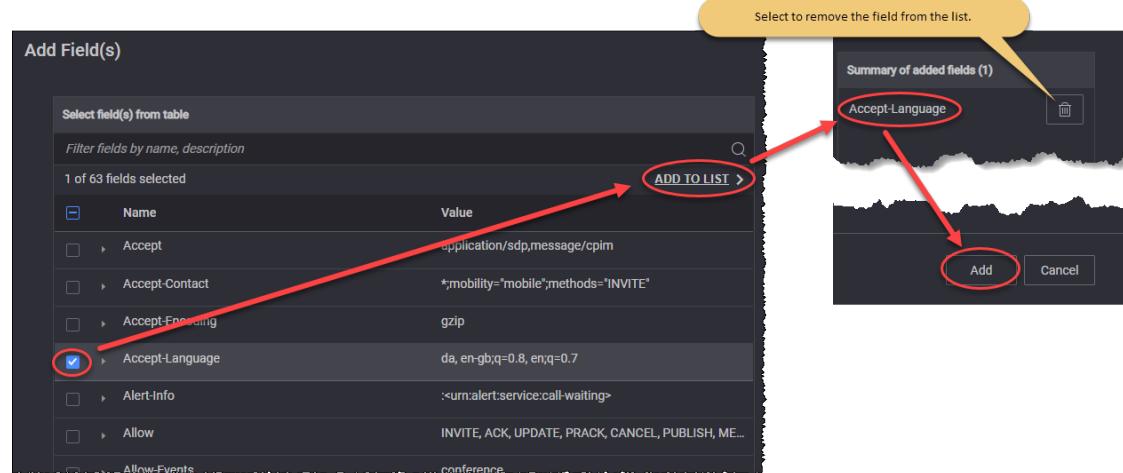
- Edit the custom header by selecting the **Message Type** from the drop-down list: **ANY, REGISTER, INVITE, ACK, BYE, OPTIONS, CANCEL, NOTIFY, SUBSCRIBE, REFER, MESSAGE, INFO, UPDATE, PRACK, RESPONSE, 1xx, 2xx**.
- Add custom header fields:
  - Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



The following custom header are available:

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

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
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

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
	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"> <li>• <b>Digest MD5</b></li> <li>• <b>AKAv1</b></li> <li>• <b>AKAv2</b></li> <li>• <b>ProxyDefined</b></li> </ul>

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

## 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 <b>Video OTT</b> .
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).
<i>OTT Servers:</i>	
	Select this button to add an OTT server to your test configuration.

Parameter	Description
	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"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Streams</a> (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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"> <li>• <b>Real</b></li> <li>• <b>Synthetic</b></li> </ul>
Protocol	Select the protocol from the drop-down list:

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>Apple HLS</b></li> <li>• <b>DASH</b></li> </ul> <p>If the stream type is set to <b>Synthetic</b>, you can choose one protocol from list. If the stream type is set to <b>Real</b>, you will see the protocol of real stream loaded.</p>
Stream Duration	<p>If the stream type is set to <b>Synthetic</b>, you can configure the stream duration in seconds. If the stream type is set to <b>Real</b>, you will see the real stream duration.</p>
Segment Duration	<p>If the stream type is set to <b>Synthetic</b>, you can configure the segment duration in seconds. If the stream type is set to <b>Real</b>, you will see the real segment duration.</p>
<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: <b>QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K</b> .
Frames per second	Set the number of frames per second.

## Custom Parameters

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

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

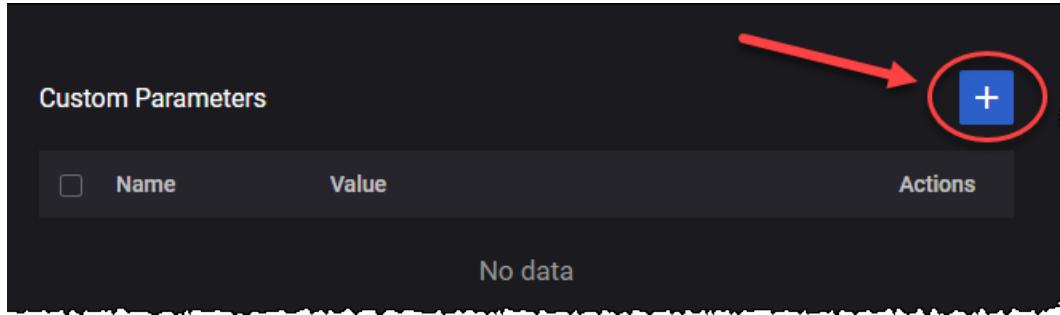
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

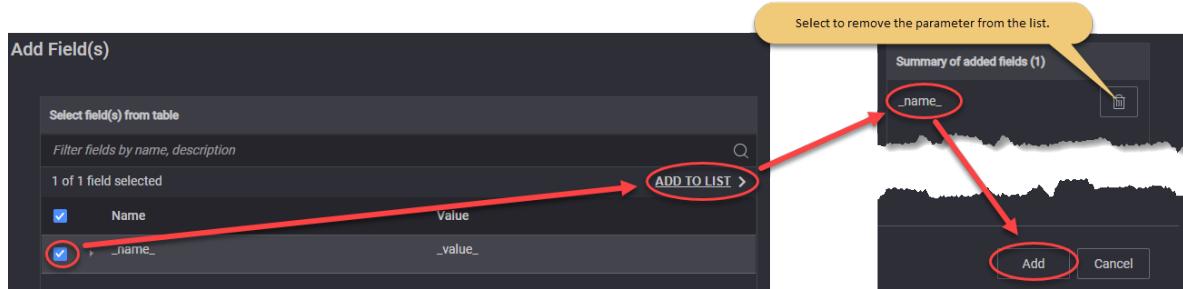
2. Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



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

## DNS Server Traffic

The following table describes the DNS Server Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>DNS Server</b> .
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>	

Parameter	Description
	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	Refer to <a href="#">Zone Manager</a> for descriptions of the DNS server zones settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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.

Parameter	Description
Type	Select the type from the drop-down list. The available options are: <ul style="list-style-type: none"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
Hostname	Set the hostname.
Address	Provide the address.

## Custom Parameters

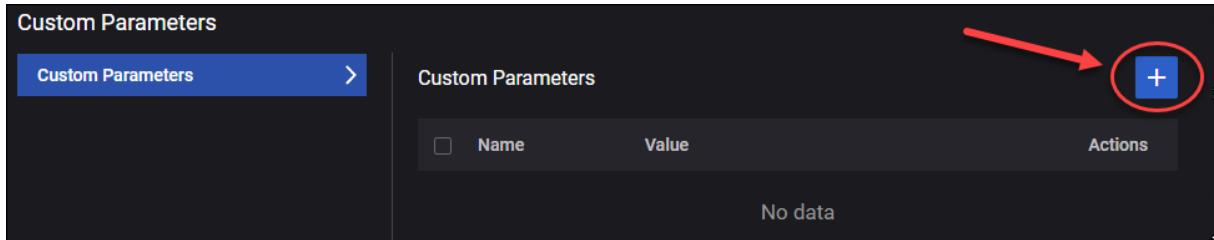
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

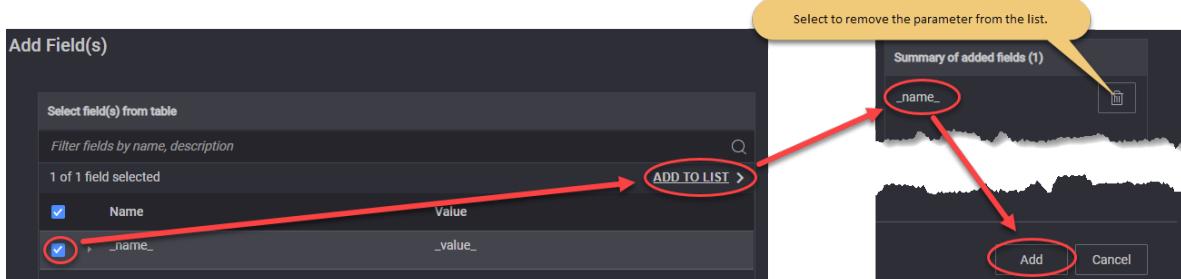
2. Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**



## Capture Replay

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b> (option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (option enabled).

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: <b>Initiator</b> and <b>Responder</b> . Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> .

Parameter	Description
	(option disabled).
Override IP Address	Select the toggle button to enable it. When enabled, Source IP Address and Source IP Address Count fields become available.
Source IP Address	The source IP address to place in the IP packet.
Source IP Address Count	The source IP address count value.

## Synthetic

The following table describes the Synthetic parameters.

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

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

The following table describes the Traffic Flow parameters.

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

## UDG

The following table describes the UDG parameters.

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

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

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

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

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

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

Parameter	Description
Address	
Port	Set the used port.

## Data/Video Throttling settings

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

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

**NOTE**

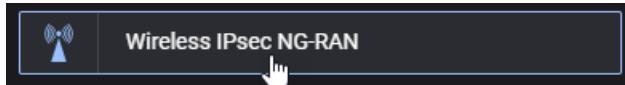
The throttling options only work for interfaces that are running IxStack, either over DPDK or over raw sockets, depending on where the traffic is terminated (if agent is present on DN/SGi server then its N6 interface should be IxStack; if there is no agent on DN/SGi, than N3 interface should be IxStack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

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

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

*CHAPTER 11***IPsec NG-RAN tests: configuration settings**

This section provides descriptions of the configuration settings that are specific to the **Wireless IPsec NG-RAN** test type:

**Topics:**

<b>Global Settings .....</b>	<b>1002</b>
Global Settings panel .....	1003
Node Start/Stop Rates .....	1004
DNS Settings .....	1004
Advanced Settings .....	1005
DNNs panel .....	1008
DNN configuration settings .....	1008
Session AMBR configuration settings .....	1012
ePCO configuration settings .....	1012
Traffic Control Settings configuration .....	1014
Impairment .....	1015
QoS Flows panel .....	1016
QoS Flow configuration settings .....	1016
QoS Flow Packet Filter configuration settings .....	1020
QoS Flow Max Packet Loss Rate settings .....	1021
QoS Flow ARP configuration settings .....	1021
QoS Flow MBR configuration settings .....	1022
QoS Flow GBR configuration settings .....	1022
Milenage .....	1022
Customer Parameters .....	1023
CA Certificates .....	1023
External Stats Server .....	1024
Global Playlists .....	1031
<b>UE configuration settings .....</b>	<b>1031</b>
UE Ranges panel .....	1032

UE Range panel .....	1033
Range Settings .....	1034
UE Identification settings .....	1034
UE Settings settings .....	1035
UE Security settings .....	1057
UE Subscribed AMBR settings .....	1061
DNNs Config .....	1062
SMS Configuration .....	1064
Untrusted WiFi Settings .....	1065
Network Slicing settings .....	1067
UE NSSAI settings .....	1068
UDM SNSSAI Mappings .....	1069
Objectives .....	1069
Control Plane Objective .....	1069
User Plane Objectives .....	1082
<b>DN configuration settings .....</b>	<b>1130</b>
DN Ranges panel .....	1131
DN Range panel .....	1131
DN N6 interface settings .....	1132
DN routes settings .....	1133
DN User Plane .....	1134
DN Stateless UDP Traffic .....	1135
DN Data Traffic .....	1137
DN Voice Traffic .....	1139
DN Video OTT Traffic .....	1150
DN DNS Server Traffic .....	1153
DN Predefined Applications Traffic .....	1156
DN Capture Replay .....	1156
DN Synthetic .....	1158
DN Throttling settings .....	1160
<b>IMS configuration settings .....</b>	<b>1160</b>
CSCF Range panel .....	1161

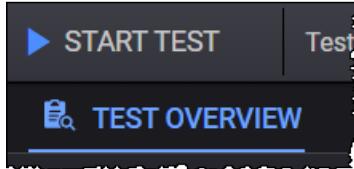
Media Function Range panel .....	1162
<b>RAN/Untrusted AP configuration settings .....</b>	<b>1162</b>
gNodeB .....	1163
gNodeB Ranges panel .....	1163
gNodeB Range settings .....	1167
gNodeB node settings .....	1168
gNodeB NSSAI settings .....	1170
gNodeB N2 interface settings .....	1172
gNodeB N3 interface settings .....	1176
eNodeB .....	1180
eNodeB Ranges panel .....	1180
eNodeB Range Settings .....	1184
eNodeB Node Settings .....	1185
S1-U Interface Settings .....	1186
S1-MME Interface Settings .....	1187
UNAP .....	1190
UNAP Ranges panel .....	1190
UNAP Range Settings .....	1191
Passthrough interface settings .....	1193
<b>SEG/N3IWF &amp; Core configuration settings .....</b>	<b>1195</b>
Core settings .....	1195
N6/SGi interface settings .....	1197
Core Ranges settings .....	1198
AMF Ranges configuration settings .....	1198
UPF Ranges configuration settings .....	1208
MME Ranges configuration settings .....	1210
SGW Ranges configuration settings .....	1219
SEG Ranges configuration settings .....	1222
SEG interface settings .....	1226
N3IWF Ranges configuration settings .....	1226
N3IWF interface settings .....	1233

## 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:

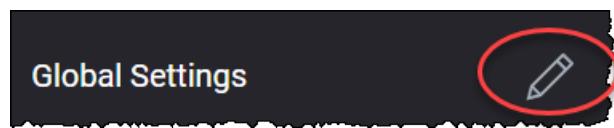


- Access and configure the following settings:

<b>Global Settings panel</b>	<b>1003</b>
<b>Node Start/Stop Rates</b>	<b>1004</b>
<b>DNS Settings</b>	<b>1004</b>
<b>Advanced Settings</b>	<b>1005</b>
<b>DNNs panel</b>	<b>1008</b>
DNN configuration settings	1008
Session AMBR configuration settings	1012
ePCO configuration settings	1012
Traffic Control Settings configuration	1014
<b>Impairment</b>	<b>1015</b>
<b>QoS Flows panel</b>	<b>1016</b>
QoS Flow configuration settings	1016
QoS Flow Packet Filter configuration settings	1020
QoS Flow Max Packet Loss Rate settings	1021

QoS Flow ARP configuration settings .....	1021
QoS Flow MBR configuration settings .....	1022
QoS Flow GBR configuration settings .....	1022
<b>Milenage .....</b>	<b>1022</b>
<b>Customer Parameters .....</b>	<b>1023</b>
<b>CA Certificates .....</b>	<b>1023</b>
<b>External Stats Server .....</b>	<b>1024</b>
<b>Global Playlists .....</b>	<b>1031</b>

## 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 <a href="#">Node Start/Stop Rates</a> .
DNS Settings	For more details, refer to <a href="#">DNS Settings</a> .
Advanced Settings	For more details, refer to <a href="#">Advanced Settings</a> .
DNNs	For more details, refer to <a href="#">DNNs</a> .
Impairment	For more details, refer to <a href="#">Impairment</a> .
QoS Flows	For more details, refer to <a href="#">QoS Flows</a> .
Override Milenage	For more details, refer to <a href="#">Milenage</a> .
Custom Parameters	For more details, refer to <a href="#">Custom Parameters</a> .
CA Certificates	For more details, refer to <a href="#">CA Certificates</a> .
External Stats Server	For more details, refer to <a href="#">External Stats Server</a> .
Global Playlists	For more details, refer to <a href="#">Global Playlists</a> .

## Node Start/Stop Rates

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

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

The DNS information is used only for the user plane path, that is, the configured DNS Server is used to resolve the destination configured for the user plane objectives in case the destination is a host name and not an IP.

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 <b>Add DNS Name Server</b> button to add a new DNS server to your test configuration. Set the IP address of the DNS server.
	Select the <b>Delete</b> button to remove the DNS server from your test configuration.

## Advanced Settings

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

Setting	Description
Overwrite Capture Size	Enable this option to overwrite the capture size for IxStack.
Custom Capture Size	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.
Power Saver on Agents	Select this option to disable the IxStack/DPDK at the end of each test on all agents.
Enable Per UE Stats	Select this option to enable per UE statistics.
Enable per PDU Session Stats	Select this option to enable per PDU Session statistics.
Enable Per QoS Flow Stats	Select this option to enable per QoS Flow statistics.
Enable Control Plane Advanced Stats	Select this option to enable control plane latency statistics.
Enable User Plane Advanced Stats	Select an option from the drill-down list for the user plane advanced statistics: <ul style="list-style-type: none"> <li>• <b>None</b> - no advanced statistics enabled.</li> <li>• <b>One Way Delay</b> - the time spent by the packet on the network from the moment it is sent until it is received.</li> <li>• <b>Delay Variation Jitter</b> - the per polling interval average delay variation jitter value calculated for all packets.</li> </ul>
Automated Polling Interval	This option is enabled by default. The statistics are retrieved based on a predefined polling interval.
Custom Polling Interval (sec)	This option becomes available only when <i>Automated Polling Interval</i> option is disabled.

Setting	Description
	It allows you to create a custom polling interval.
Log Level	Select one of the options: <ul style="list-style-type: none"> <li><b>Info</b> - Designates informational messages that highlight the progress of the application at coarse-grained level.</li> <li><b>Debug</b> - Designates fine-grained informational events that are most useful to debug the application.</li> </ul>
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 <a href="#">here</a>.</i>
Response Cache Settings	<i>The settings are described <a href="#">here</a>.</i>
Ignore Offline Agents At Runtime	When this option is enabled, if an agent loses connection to the Middleware during a test, the test will not stop but continue without that agent.

## Traffic Settings

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

Setting	Description
<i>GTPU Source Port:</i>	
Start	Indicates the source port for the GTPU tunnel. By default, the registered UDP port for GTPU is 2152.
Count	Set the count value.
<i>Reserved cores for RTP Tx:</i>	
Enable RTP	Select this option to enable RTP.
Cores	The number of cores reserved for RTP transmission.
<i>Traffic Control</i>	
Traffic Control	Set the traffic control port. By default, it is set to 44556.

<b>Setting</b>	<b>Description</b>
Port	
Enable Jumbo Frame	<p>Enable this option if your test traffic requires the use of jumbo frames (Ethernet frames with more than 1500 bytes of payload).</p> <p>When you enable this option, you can then configure any of the MTU parameters in the test to any valid jumbo frame size (up to 9,000 bytes).</p>
Enable IxStack L4 Port Randomization	Select this option to enable IxStack L4 Port Randomization.
Enable UDP Port Recycling	Select this option to enable IxStack UDP Port Recycling.
Enable TCP Port Recycling	Select this option to enable IxStack TCP Port Recycling.
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).

## Response Cache Settings

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

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

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

<b>Setting</b>	<b>Description</b>
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:

<b>DNN configuration settings</b>	.....	<b>1008</b>
<b>Session AMBR configuration settings</b>	.....	<b>1012</b>
<b>ePCO configuration settings</b>	.....	<b>1012</b>
<b>Traffic Control Settings configuration</b>	.....	<b>1014</b>

### 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"> <li>• A mandatory Network Identifier that defines the external network to which the UPF is connected.</li> <li>• An optional Operator Identifier that defines the PLMN backbone in which the UPF is located.</li> </ul> <p>A 5GS Data Network Name (DNN) is equivalent to an EPS APN. It is a reference to a data network, and it may be used to select an SMF or UPF for a PDU session and to determine policies applicable to the PDU session.</p>

Setting	Description
	<p>The DNN field supports dynamic values. These values can be obtained with a sequence generator.</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><b>NOTE</b> 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"> <li>• <code>dnn[4-9, ]</code> an implicit increment of 1 is used</li> <li>• <code>dnn[4-9]</code> as above</li> <li>• <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</li> <li>• <code>dnn[4-, ]</code> as above</li> <li>• <code>dnn[4- ]</code> as above</li> <li>• <code>dnn[4]</code> as above</li> </ul> <p>UEs will use the DNN values from the pool in a round robin manner.</p> <p><b>IMPORTANT</b> If multiple sequence generators are configured and their pools overlap (for example: <code>dnn[000-600,1].keysight.com</code> <code>dnn[500-999,1].keysight.com</code>), for UEs that use the second DNN pool, the DNN generated values might not be allocated starting with the start_value (they might start with an intermediate value in the second pool).</p>
PDU Type	Select the desired PDU type: IPv4, IPv6 or IPv4v6.
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 <a href="#">QoS Flow configuration settings</a>.</p>

<b>Setting</b>	<b>Description</b>
Allowed SSC Modes	<p>Session and Service Continuity (SSC) Mode for this DNN:</p> <ul style="list-style-type: none"> <li>• <b>SSC Mode 1:</b> The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved.</li> <li>• <b>SSC Mode 2:</b> 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.</li> <li>• <b>SSC Mode 3:</b> 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.</li> </ul>
Default SSC Mode	<p>Select the desired default SSC mode for this DNN.</p> <p>The SSC mode associated with a PDU Session does not change during the lifetime of a PDU Session.</p>
Allowed Services	<p>Select the allowed services from the drop-down list: Service 1, Service 2, Service 3, or all. In the 5G System, the <i>allowed services</i> may comprise any number of service identifiers allowed for the subscriber in the PDU Session. The PCF maps those service identifiers into PCC rules according to local configuration and operator policies.</p>
Subscription Categories	<p>Select the desired Subscription Category for this range of UEs.</p> <p>Subscriber Category is an information type structured as a list of category identifiers associated with a subscriber. It may comprise any number of identifiers associated with the subscriber (such as platinum, gold, silver, bronze).</p>
IPv4 Index	<p>The IPv4 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv4 addresses.</p>
IPv6 Index	<p>The IPv6 Index value for the PDU sessions accessing this DNN. This value identifies the IP address allocation method for IPv6 addresses.</p>
EPS Interworking	<p>Enable this option if the UE subscription data indicates support for interworking with EPS for this DNN.</p>
ADC Support	<p>Enable this option if the DNN will support PDU sessions in which application detection and control (ADC) is enabled for subscribers.</p>
Subscriber Spending Limits	<p>Enable this option if the DNN will support PDU session policies that are based on subscriber spending limits.</p>
Offline	<p>Enable this option if the DNN will support the offline charging method for PDUs sessions.</p>

<b>Setting</b>	<b>Description</b>
Online	Enable this option if the DNN will support the online charging method for PDUs sessions.
Is Emergency DNN	When this option is enabled, if an UE range has mapped this type of DNN, it will perform an emergency PDU Session.
MPS Priority	Enable this option if the DNN will support subscription to MPS priority service. The priority applies to all traffic on the PDU Session.
Dual Registration Mode	When enabled, it transfers this session to the other RAT in dual registration mode. If the session does not exist, it will be created in the other RAT.
MPS Priority Level	Specify the Multimedia Priority Services (MPS) priority level. This is the relative priority level for MPS.
IMS Signaling Priority	Specify the IP Multimedia Subsystem (IMS) signaling priority. This value indicates subscription to IMS signaling priority service. The priority applies only to IMS signaling traffic.
Access Network Instance	<p>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.</p>
Core Network Instance	<p>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.</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.
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 <a href="#">Session AMBR configuration settings</a>.</i>
ePCO	<i>Select this option to open the extended protocol configuration options panel. These settings are described in <a href="#">ePCO configuration settings</a>.</i>
Traffic Control Settings	<i>Select this option to open the traffic control settings panel. These settings are described in <a href="#">Traffic Control Settings configuration</a>.</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

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

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

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

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

Known limitations:

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

## Traffic Control Settings configuration

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

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

The following tables describes the Traffic Control Settings parameters.

Parameter	Description
Traffic Control Settings	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: •  - Select to add the remote IPv4 address.

Parameter	Description
	<ul style="list-style-type: none"> <li> - Select to remove the remote IPv4 address.</li> </ul>
Remote IPv6	<p>Select:</p> <ul style="list-style-type: none"> <li> - Select to add the remote IPv6 address.</li> <li> - Select to remove the remote IPv6 address.</li> </ul>

## Impairment

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

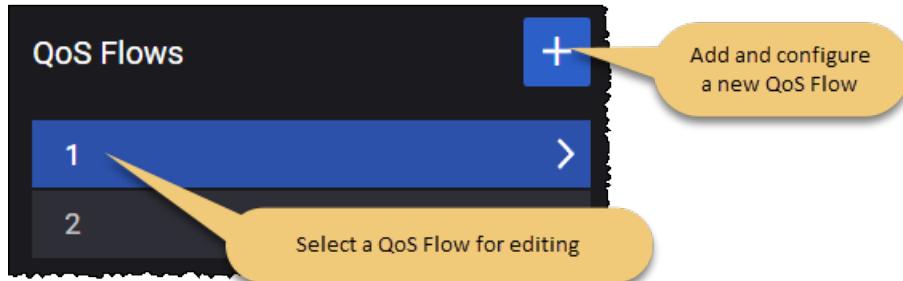
Setting	Description
<i>Impairment Profiles:</i>	
	Select the <b>Add impairment profile</b> button to add a new profile to your test configuration.
<i>Impairment Profile:</i>	
	Select the <b>Delete impairment profile</b> button to remove the profile from your test configuration.
Name	Each impairment profile 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: <b>Custom script</b> .
Script file	This parameter is available only when <b>Action Type</b> is set to <b>Custom script</b> . It allows you to add a custom script, using the <b>Upload</b> button. To remove the script, select the <b>Clear</b> 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:

<b>QoS Flow configuration settings</b>	<b>1016</b>
<b>QoS Flow Packet Filter configuration settings</b>	<b>1020</b>
<b>QoS Flow Max Packet Loss Rate settings</b>	<b>1021</b>
<b>QoS Flow ARP configuration settings</b>	<b>1021</b>
<b>QoS Flow MBR configuration settings</b>	<b>1022</b>
<b>QoS Flow GBR configuration settings</b>	<b>1022</b>

### 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><b>IMPORTANT</b> This parameter is available only if the <a href="#">Is Default</a> option is not selected.</p> <p>The following options are available:</p> <ul style="list-style-type: none"> <li>• <b>Data</b> - 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.</li> <li>• <b>Audio</b> - LoadCorePCF/PCRF needs information related to this flow/bearer from CSCF.</li> <li>• <b>Video</b> - LoadCorePCF/PCRF needs information related to this flow/bearer from CSCF.</li> </ul>
Network Initiated Flow	<p><b>IMPORTANT</b> This parameter is available only if the <a href="#">Is Default</a> 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"> <li>• <i>Delay After Initial Registration (s)</i> - set the value for this parameter.</li> <li>• <i>Interval between Create and Delete (s)</i> - set the value for this parameter.</li> <li>• <i>Iterations</i> - set the value for this parameter.</li> </ul>
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 (non-GBR), 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>

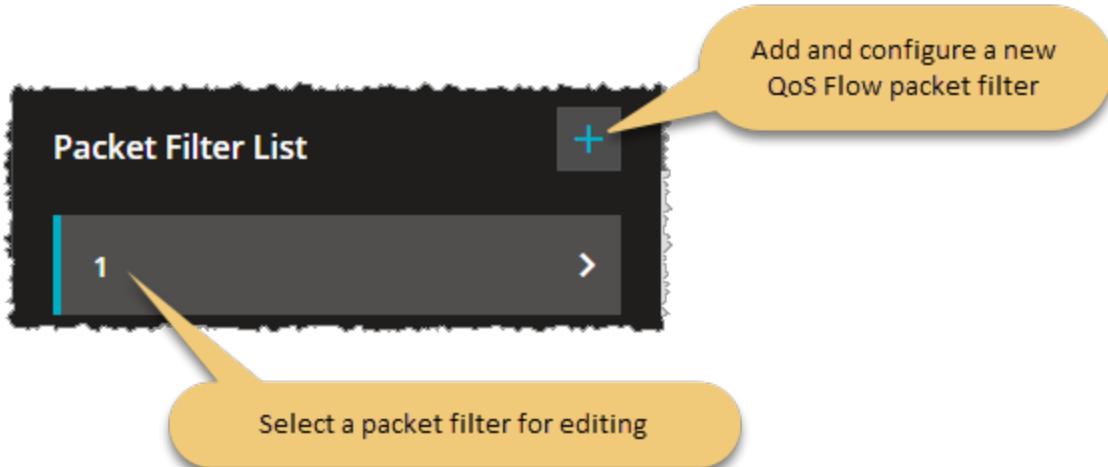
<b>Setting</b>	<b>Description</b>
	milliseconds) over which the GFBR and MFBR are calculated.
QoS Rule Precedence	<p>Specify the desired QoS Rule Precedence value for this QFI.</p> <p>The QoS rule precedence value (and the PDR precedence value) determine the order in which a QoS rule or a PDR, respectively, 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><b>NOTE</b> 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><b>IMPORTANT</b> This is available if <a href="#">Is Default</a> option is enabled.</p> <p>If this option is not enabled, a new <a href="#">Packet Filter List</a> 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.

<b>Setting</b>	<b>Description</b>
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	<p>If needed, enable this option.</p> <p>This option is part of the Option 3x and Dual Connectivity NR feature, for more details refer to <a href="#">UE Range Panel</a>.</p>
Packet Filter List	<p><b>IMPORTANT</b> This is available if <a href="#">Use Match-all Packet Filter</a> option is not selected.</p> <p>Refer to the following topic for a description of the Packet Filter configuration settings: <a href="#">QoS Flow Packet Filter configuration settings on page 141</a>.</p>
Max Packet Loss Rate	Refer to the following topic for a description of the Max Packet Loss Rate configuration settings: <a href="#">QoS Flow Maximum Packet Loss configuration settings</a> .
ARP	Refer to the following topic for a description of the ARP configuration settings: <a href="#">QoS Flow ARP configuration settings</a> .
MBR	Refer to the following topic for a description of the MBR configuration settings: <a href="#">QoS Flow MBR configuration settings</a> .
GBR	Refer to the following topic for a description of the GBR configuration settings: <a href="#">QoS Flow GBR configuration settings</a> .

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

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

## QoS Flow Max Packet Loss Rate settings

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

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

## QoS Flow ARP configuration settings

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

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

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

## QoS Flow GBR configuration settings

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

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

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

## Milenage

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

## **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
<i>CA Certificates:</i>	
	Select the <b>Add CA Certificate</b> button to add a new certificate to your test configuration.
<i>CA Certificate:</i>	
	Select the <b>Delete CA Certificate</b> 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 <b>Upload</b> button. To remove the script, select the <b>Clear</b> button.

## External Stats Server

If this option is selected, it will allow you to add an external statistic server.

The following table describes the settings required for the External Stats Server configuration.

Setting	Description
<i>External Stats Server:</i>	
Profile	This parameter allows you to upload or remove a stats server profile. Press <b>Upload</b> and load the preferred server profile, or <b>Clear</b> to dismiss one that is set.
Server Address	The address of the external stats server.

### Setting up a Profile

The External Stats Server feature allows you to forward statistic logs to an external server, thus requiring to upload a profile that defines where the stats are stored and what stats should be transferred.

**IMPORTANT** This feature is designed to support any type of external entity, but currently it supports only the Apache Kafka Plugin.

The parameters required to create the request to the external entity are configured in the **Profile** JSON file that is uploaded to Keysight Open RAN Simulators, Cloud Edition 5.1. The following structure and parameters describe the standard content of the JSON file:

Section/ Parameter	Definition	Code Sample
<i>Input section</i>	<i>Lists all the stats/config parameters used in the profile. All the parameters are already available in Keysight Open RAN Simulators, Cloud Edition 5.1. the following types are supported:</i>	

Section/ Parameter	Definition	Code Sample
stat	It can be any stat supported in Keysight Open RAN Simulators, Cloud Edition 5.1. The stats can be filtered by any other stat from the stat response.	<p>With filter sample:</p> <pre>{   "type": "stat",   "group": "AgentStatistics",   "stat": "CPU Percent",   "name": "cpu_percent1",   "filterBy": {     "stat": "agentIP",     "value": "10.38.158.83"   } }</pre> <p>Without filter sample:</p> <pre>{   "type": "stat",   "group": "Fullcoreoverview_RegisteredAttachedUE",   "stat": "UEs Registered",   "name": "no_of_UE_Registered" }</pre>
config	It can be any parameter exposed in the UI. The path is the same as the one used by the UI to set/get a parameter (see <a href="#">Parameter sample path on the next page</a> image).	<pre>{   "type": "config",   "group": "config/nodes/ausf/ranges/1/nodeSettings",   "stat": "mcc",   "name": "mcc" }</pre>
<i>Mappings section</i>	<i>Mapping will use any input parameter referred by name. Mapping also supports mathematical expressions to combine stats.</i>	
	For example, Keysight Open RAN Simulators, Cloud Edition 5.1 exposes <code>stat1</code> and <code>stat2</code> but the user needs <code>user_stat</code> which comprises $(\text{stat1} + \text{stat2}) / 100$ . The expression is evaluated and the result sent under <code>user_stat</code> name.	<ul style="list-style-type: none"> <li>one parameter sample:</li> </ul> <pre>{   "type": "controlplane",   "from": "no_of_UE_Registered",   "to": "no_of_UE_Registered" }</pre> <p>OR</p>

Section/ Parameter	Definition	Code Sample
		<pre data-bbox="804 340 1447 508"> {   "type": "controlplane",   "from": "mcc",   "to": "MCC" } </pre> <ul data-bbox="845 540 1274 572" style="list-style-type: none"> <li>• with mathematical expression:</li> </ul> <pre data-bbox="804 604 1447 804"> {   "type": "controlplane",   "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",   "to": "agent1 cpu ratio" } </pre>

## Parameter sample path



The screenshot shows a browser window with the URL <https://10.38.157.61/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings>. The response is a JSON object containing fields like instanceId, mcc, mnc, routingIndicators, links, and options.

```

{
  "instanceId": "7ea3abc7-f0f6-435b-9154-125deddd101b",
  "mcc": "226",
  "mnc": "04",
  - routingIndicators: [
    1234,
    2222
  ],
  - links: [
    - {
      rel: "self",
      type: "self",
      method: "GET",
      href: "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings"
    },
    - {
      rel: "meta",
      type: "meta",
      method: "GET",
      href: "/api/v2/sessions/wireless-07a05ef0-a421-4894-869d-81e6e88831aa/config/config/nodes/ausf/ranges/1/nodeSettings/$options"
    }
  ]
}

```

## Sample profile

```

{
  "profile": {
    "type": "kafka",
    "3gpp_scenario": "QUIC_ABR_DEBUG",
    "event_type": "ATTS_TOOLS_KEYSIGHT_EVENT",
    "specversion": "1.1",
    "kafkatopics": "com.att.ant.stage.ATTSSKeysight.1.0",
    "kafkaschemaUrl": "https%3A%2F%2Fc1001.eastus2.uat.iebus.3pc.att.com%3A8082%2Fschemas%2Fids%2F6635&schemaId=14260",
  }
}

```

```

"kafkaHeaderBootstrapUrl": "cl001.eastus2.uat.iebus.3pc.att.com:9093",
"kafkaHeaderSaslMechanism": "PLAIN",
"kafkaHeaderOAuthScope": "ANT-data-feed-dev-stage",
"kafkaUsername": "m30317@ant.att.com",
"kafkaPassword": "August2023#",
"input": [
    {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent1",
        "filterBy": {
            "stat": "agentIP",
            "value": "10.38.158.83"
        }
    },
    {
        "type": "stat",
        "group": "AgentStatistics",
        "stat": "CPU Percent",
        "name": "cpu_percent2",
        "filterBy": {
            "stat": "agentIP",
            "value": "10.38.157.97"
        }
    },
    {
        "type": "config",
        "group": "config/nodes/ausf/ranges/1/nodeSettings",
        "stat": "mcc",
        "name": "mcc"
    },
    {
        "type": "config",
        "group": "config/nodes/ue/ranges/1/userPlane/tigerObjective/1/statelessUDP",
        "stat": "ipAddress",
        "name": "ipAddress"
    },
    {
        "type": "stat",
        "group": "Fullcoreoverview_RegisteredAttachedUE",
        "stat": "UEs Registered",
        "name": "no_of_UE_Registered"
    },
    {
        "type": "stat",
        "group": "Fullcoreoverview_PDUSessionEstablishment",
        "stat": "PDU Session Establishment Succeeded",
        "name": "no_of_PDU_Session_Established"
    },
]

```

```
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
  "stat": "L2-3 Device Rx Traffic",
  "name": "L3 Server::Total Bits/Sec"
},
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_UserPlaneThroughput",
  "stat": "L2-3 Device Tx Traffic",
  "name": "L3 Client::Total Bits/Sec"
},
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_TCPConnections",
  "stat": "TCP connections established",
  "name": "HTTP/s Handshakes Succeeded"
},
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_TCPConnections",
  "stat": "TCP connect failed",
  "name": "HTTP/s Handshakes Failed"
},
{
  "type": "stat",
  "group": "Fullcoreapplicationtraffic_TCPConnections",
  "stat": "TCP connections closed normally",
  "name": "HTTP/s Connection Closed"
}
],
"mappings": [
  {
    "type": "controlplane",
    "from": "cpu_percent1 + cpu_percent2",
    "to": "total cpu_percent %"
  },
  {
    "type": "controlplane",
    "from": "cpu_percent1/(cpu_percent1 + cpu_percent2)",
    "to": "agent1 cpu ratio"
  },
  {
    "type": "controlplane",
    "from": "cpu_percent2/(cpu_percent1 + cpu_percent2)",
    "to": "agent2 cpu ratio"
  },
  {
    "type": "controlplane",
    "from": "mcc",
    "to": "MCC"
  }
]
```

```

},
{
  "type": "controlplane",
  "from": "ipAddress",
  "to": "Destination IP Address"
},
{
  "type": "controlplane",
  "from": "no_of_UE_Registered",
  "to": "no_of_UE_Registered"
},
{
  "type": "controlplane",
  "from": "no_of_PDU_Session_Established",
  "to": "no_of_PDU_Session_Established"
},
{
  "type": "userplane",
  "from": "L3 Server::Total Bits/Sec",
  "to": "L3 Server::Total Bits/Sec"
},
{
  "type": "userplane",
  "from": "L3 Client::Total Bits/Sec",
  "to": "L3 Client::Total Bits/Sec"
},
{
  "type": "userplane",
  "from": "HTTP/s Handshakes Succeeded",
  "to": "HTTP/s Handshakes Succeeded"
},
{
  "type": "userplane",
  "from": "HTTP/s Handshakes Failed",
  "to": "HTTP/s Handshakes Failed"
},
{
  "type": "userplane",
  "from": "HTTP/s Connection Closed",
  "to": "HTTP/s Connection Closed"
}
]
}
}

```

**Event body sent to Kafka**

```
[
{
  "eventBody": {

```

```

"id": "wireless-0acbc45b-8777-4250-a3ec-4f00e47399c8_39",
"time": "2024-02-29T13:57:35Z",
"type": "ATTS-TOOLS-KEYSIGHT-EVENT",
"specversion": "1.1",
"source": "https://10.38.157.61/wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
"datacontenttype": "application/json",
"payload": [
    {
        "type": "resource_info",
        "resource_info": {
            "simulated_tool_info": [
                {
                    "tool_name": "LoadCore",
                    "middleware_ip": "10.38.157.61"
                }
            ],
            "network_type": "5G",
            "3gpp_scenario": "QUIC_ABR_DEBUG"
        }
    },
    {
        "type": "test_execution_result",
        "test_execution_result": {
            "control_plane_result": {
                "Destination IP Address": "20.0.6.10",
                "MCC": "226",
                "agent1 cpu ratio": "0.455321",
                "agent2 cpu ratio": "0.544679",
                "no_of_PDU_Session_Established": "100",
                "no_of_UE_Registered": "0",
                "total cpu_percent %": "3.0902"
            },
            "userplane_plane_result": {
                "L3 Client::Total Bits/Sec": "0",
                "L3 Server::Total Bits/Sec": "0"
            }
        }
    },
    {
        "type": "test_execution_details",
        "test_execution_details": {
            "testName": "4 - Full Core Base Config",
            "testSessionID": "wireless-07a05ef0-a421-4894-869d-81e6e88831aa",
            "UserID": "admin@example.org",
            "testStatus": "STOPPING",
            "testStartTime": "2024-02-29T13:55:40Z",
            "testDuration": 105,
            "testStopTime": "2024-02-29T13:57:31Z"
        }
    }
]

```

```

        ],
    },
    "payloadType": "JSON",
    "value": {}
}
]

```

## Global Playlists

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

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

<b>UE Ranges panel</b> .....	<b>1032</b>
<b>UE Range panel</b> .....	<b>1033</b>
<b>Range Settings</b> .....	<b>1034</b>
UE Identification settings .....	1034
UE Settings settings .....	1035
UE Security settings .....	1057

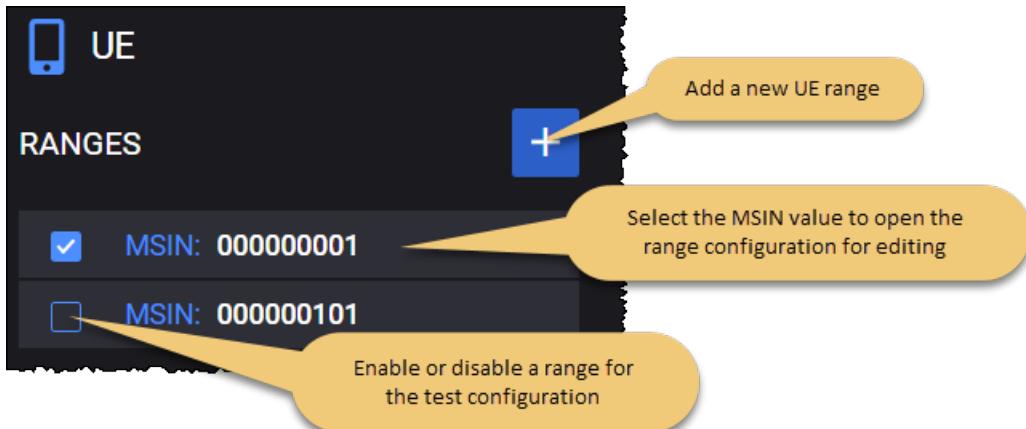
UE Subscribed AMBR settings .....	1061
DNNs Config .....	1062
SMS Configuration .....	1064
Untrusted WiFi Settings .....	1065
<b>Network Slicing settings .....</b>	<b>1067</b>
UE NSSAI settings .....	1068
UDM SNSSAI Mappings .....	1069
<b>Objectives .....</b>	<b>1069</b>
Control Plane Objective .....	1069
User Plane Objectives .....	1082

## 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 ...



If multiple agents are assigned to the UE, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **All UE Ranges and RAN Ranges on All Agents** - for example, for a test with 2 agents and 2 UE ranges and 2 RAN ranges, UE range1 and UE range2 and their parent ranges as well as all RAN ranges part of Mobility Path, and Secondary RAN ranges will be distributed to both agent1 and agent2.
- **Round Robin UE Ranges and RAN Ranges per Agent** - for example, if UE range1 is distributed to agent1, parent RAN range as well as all RAN ranges part of the Mobility Path (visited gNB/eNB ranges) and the Secondary RAN ranges will also be distributed on agent1.

## UE Range panel

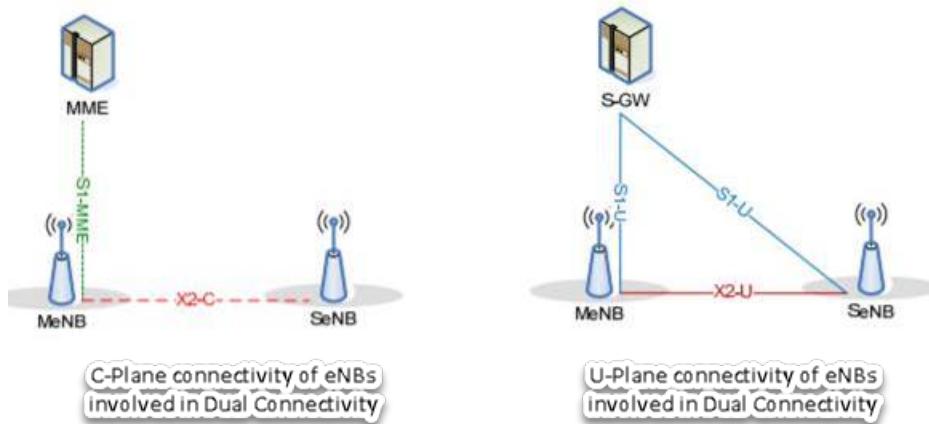
When you select an MSIN from the UE **Ranges** panel, LoadCore opens the **Range** panel, from which you can:

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

## UE range controls and settings

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

## Range Settings

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

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

<b>UE Identification settings</b>	<b>1034</b>
<b>UE Settings settings</b>	<b>1035</b>
<b>UE Security settings</b>	<b>1057</b>
<b>UE Subscribed AMBR settings</b>	<b>1061</b>
<b>DNNs Config</b>	<b>1062</b>
<b>SMS Configuration</b>	<b>1064</b>
<b>Untrusted WiFi Settings</b>	<b>1065</b>

### 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**.

<b>Setting</b>	<b>Description</b>
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	<p>The MSIN value that will be assigned to the first simulated UE in the range.</p> <p><b>About MSIN ...</b></p> <p>The Mobile Subscriber Identification Number (MSIN) is a number that a wireless operator uses to uniquely identify a mobile phone. It is—at most—10-digits long. The MSIN is used (in combination with the MCC and MNC) to form the International Mobile Subscriber Identity (IMSI) number.</p>
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 Settings settings

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

<b>Setting</b>	<b>Description</b>
<i>Settings:</i>	
Dual Registration Mode	<p>When enabled, this option allows an UE to be registered/attached in the same time to 5GS via a gNodeB and to EPS via an eNodeB.</p> <p>The UE will activate this feature in case:</p>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>Dual Registration Mode option is enabled.</li> <li>At least one DNN has <a href="#">Dual Registration Mode</a> option enabled.</li> <li>It has a <a href="#">parent gNodeB</a> (<i>gNodeB-1</i> for example).</li> <li>It has a Handover objective configured with <a href="#">visited nodes</a> (for example, primary node <i>gNodeB-1</i> and secondary node <i>eNodeB-1</i>).</li> </ul>
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>
Subscriber 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 DonwlinkNASTransport/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/Periodic Tracking Area Update	<p>By default, this option is not enabled.</p> <p>If the periodic registration / TAU functionality is disabled, the UE will ignore the T3512/T3412 timer received in the Registration Accept/TAU</p>

<b>Setting</b>	<b>Description</b>
	<p>Accept and will not send any Periodic Registration Update/Tracking Area Update request.</p> <p>During the Initial Registration/Initial Attach, the AMF/MME sends in the Registration Accept/Attach Accept a T3512/T3412 timer, which consists of a Unit-Value pair. For example, a value of 30 and unit of 10min means 300 minutes.</p> <p>The T3512/T3412 timer can be overridden by subsequent Registration Accept/TAU Accept messages. If T3512/T3412 is 0 or Disabled, no periodic registration/periodic TAU should be performed. If no T3512/T3412 value is present in the Registration Accept /Attach Accept message, the last known T3512/T3412 value is used. If a T3512/T3412 was never transmitted by the AMF/MME, the default value of 54 minutes will be used.</p> <p>The T3512/T3412 timer is triggered when the UE enters idle. If the UE exits the idle state, the T3512/T3412 timer is stopped. When the UE enters again in idle, the T3512/T3412 timer is restarted.</p> <p>While the UE is in idle mode, when the T3512/T3412 timer expires:</p> <ul style="list-style-type: none"> <li>• If the UE is not registered/attached for emergency services, the UE initiates a Periodic Registration Update/Tracking Area Update procedure and restarts the T3512/T3412 timer.</li> <li>• If the UE is registered/attached for emergency services, the UE locally de-registers/detaches and the AMF/MME locally detaches the UE.</li> </ul>
Include UEContextRequest IE for PRU Initial UE Message	<p>If enabled, it will include the UEContextRequest IE for the PRU Initial UE Message.</p> <p><b>IMPORTANT</b> This option appears only if <b>Enable Periodic Registration Update/Periodic Tracking Area Update</b> is enabled.</p>
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 Router Solicitation (ms)	The time (in milliseconds) that will elapse before the UE sends an ICMPv6 Router Solicitation message (a <b>0</b> value means no delay). If, during this time, the UE receives an unsolicited Router Advertisement, the sending of the Router Solicitation will be canceled.
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.
Check AUTN	By default, this option is disabled.

<b>Setting</b>	<b>Description</b>
	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.
Unsolicited Router Advertisement	Select to enable this option.
AMF Force Identification During Registration	This option will force the AMF to always trigger the "Identification Procedure" to get the identity of the UE. When the NG-RAN node receives this request, it responds with the IMEISV or the SUCI.
Identity Request PEI Type	When the Identification Procedure is triggered by the MME/AMF due to the <a href="#">AMF Force Identification During Registration</a> option being enabled, it allows the selection of the requested PEI type: <b>IMEISV</b> or <b>IMEI</b> . Default value: <b>IMEISV</b> .
Send Registration Accept in Initial Context Setup Request	If enabled, the UE will send Registration Accept in Initial Context Setup Request.
Always Include Uplink Data Status IE in Service Request Message	The UE will always include the Uplink Data Status IE for a Service Request message, not only if it has pending data.
Enable Passthrough	Select this option to enable passthrough and any interface. Applicable to all passthrough topologies (UE/gNB or UPF). Applicable to either direction: GTPu to IP or/and IP to GTPu.
Attach/Register with GUTI	When the Primary Objective type is Subscribers Per Second, enabling this option will trigger a Registration/Attach Request with the type of user identity set to temporary identity (GUTI). When option is not enabled, the type of user identity in the Registration/Attach Request will be permanent identity.
Authentication with GUTI	This option is available only when Attach/Register with GUTI option is enabled. When enabled, this option triggers authentication in case of attach (4G)/register (5G) with GUTI.
Force Emergency Registration	When this option is enabled, the UE will perform an Emergency registration (instead of Initial Registration). 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

<b>Setting</b>	<b>Description</b>
	Emergency Registration will not be performed even if there is a Secondary Objective that uses an emergency DNN.
Identity Type for Emergency Registration	<p>Select the identity type to use from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>SUCI/IMSI</b> - where SUCI is used for 5G network, and IMSI for 4G network</li> <li>• <b>IMEISV/IMEI</b> - where IMEISV is used for 5G network, and IMEI for 4G network.</li> <li>• <b>IMEI</b> - where IMEI is used for 5G networks</li> </ul>
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"> <li>• <b>Never</b>: Authentication is not performed during mobility registration.</li> <li>• <b>Always</b>: Authentication during mobility registration is always performed.</li> <li>• <b>No Native Context</b>: Authentication during mobility registration is performed only when the UE does not hold a native 5G security context.</li> </ul>
Update GUTI in TAU	Select to enable this option.
Access Class	<p>Select the Access Class of the UE from the drop-down list. The following options are available: <i>None</i>, <i>Low Priority Access</i>, <i>11 - For PLMN Use</i>, <i>12 - Security Service</i>, <i>13 - Public Utilities</i>, <i>14 - Emergency Services</i>, <i>15 - PLMN Staff</i>.</p> <p><b>IMPORTANT</b> This option is available for 4G only.</p>
Index to RFSP	Set the value for the initial Context Setup Request - Index to RFSP IE. Possible values are in range of 0 to 256, where a zero value means the <i>indexToRFSP</i> is not sent.
GUTI Reallocation Delay	The time to wait, in seconds, after the UE registers to allocate a new

<b>Setting</b>	<b>Description</b>
(s)	GUTI. A value of zero disables the reallocation.
<i>Radio Capability</i>	
UE Radio Capability IE Value for LTE	The UE radio capability IE value that will be included UE Capability Info Indication message.
UE Radio Capability IE Value for NR	The UE radio capability IE value that will be included UE Capability Info Indication message.
Send UE Capability IE Indication after Initial Context Setup	Enable this option to sent UE capability IE indication after initial context setup.
Trigger UE Radio Capability Check Procedure after Registration	This option will trigger from CoreSim the UE radio capability check procedure after registration in 5G or UE radio capability match procedure after attach in 4G.
Replay UE Radio Capability	<p>The UE Radio Capability IE is replayed in the Initial Context Setup Request and UE Radio Capability Match / Check messages on 4G and 5G. This option is applicable for the AMF and MME nodes.</p> <p><b>NOTE</b> It is not applicable for Initial Context Setup Request of an inter-RAT handover procedure.</p> <p><b>NOTE</b> After UE Radio Capability Match / UE Radio Capability Check procedures, UE always sends UE Radio Capability Info Indication.</p>
<i>Location Reporting</i>	<i>Select the check box to enable location reporting as defined in TS 23.502 (supported on the AMF and NG-RAN nodes).</i>
Reporting Type	<p>Select the value from the drop-down list. The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Direct</b> - If the test timeline is long enough, the AMF generates <i>n</i> LocationReportingControl messages at every <i>m</i> seconds from the moment Registration Complete message is received by the AMF (<i>n</i> is the value configured for <a href="#">Number of Repeats</a> and <i>m</i> is the value of <a href="#">Interval Between Requests</a>).</li> <li>• <b>Change of Serving Cell</b> - In case of Handover with AMF change, if <b>Change of Serving Cell</b> is selected, after handover, the new AMF will send a LocationReportingControl message to the NG-RAN.</li> </ul>
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

<b>Setting</b>	<b>Description</b>
	LocationReportingControl message (event-type: change-of-serving-cell).
Stop Time (Seconds)	The number of seconds since the <a href="#">Start Time</a> 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> <ul style="list-style-type: none"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul>
<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.
<i>Location Services</i>	<p>Select the check box to enable <a href="#">Location Services</a> (as described in TS23271). The Location Services procedures over the LPPa interface are detailed in TS36455.</p> <div data-bbox="561 1712 747 1776" style="background-color: #e0e0e0; padding: 5px; display: inline-block;"> <b>NOTE</b> </div> <p>When Location Services is enabled, at least 1 profile must be configured (a maximum of 15 profiles allowed).</p>

<b>Setting</b>	<b>Description</b>
<i>Reroute NAS Request</i>	<i>Select the check box to enable this option.</i>
<i>AMF Set ID</i>	<i>The AMF Set ID to use for this simulated AMF node. The Set ID uniquely identifies the AMF Set within the AMF Region.</i>
<i>Reroute After SMC</i>	<i>If selected, the AMF will reroute after Security Mode procedure.</i>
<i>NSSAI</i>	<i>See the <a href="#">NSSAI on page 1044</a> table for details.</i>
<i>Network Initiated PDU Session Modification</i>	<i>See the <a href="#">Network Initiated PDU Session Modification on page 1045</a> table for details.</i>
<i>Refresh Security Context</i>	<i>When enabled, the AMF/MME will initiate the Security Mode Control procedure to obtain a fresh uplink NAS Count which is used to generate a new Security Key.</i>
<i>Delay(s)</i>	<i>The time to wait, in seconds, before triggering the Security Mode Control procedure after the UE is registered.</i>
<i>Iterations</i>	<i>The number of times the security context will be refreshed.</i>
<i>Interval(s)</i>	<i>The time, in seconds, between two iterations.</i>
<i>Core Network Assistance Information For Inactive</i>	<p><i>If enabled, the configured Core Network Assistance Information for RRC INACTIVE IE is present only in the INITIAL CONTEXT SETUP REQUEST message carrying the initial Registration Accept. It is not present in the INITIAL CONTEXT SETUP REQUESTS carrying other types of NAS messages, UE CONTEXT MODIFICATION REQUEST, HANDOVER REQUEST or PATH SWITCH REQUEST ACKNOWLEDGE. It is not present for Emergency Registration.</i></p> <p><i>This option is disabled by default. See <a href="#">Core Network Assistance Information For Inactive</a> for configuration details.</i></p>
<i>Paging Settings</i>	<p><b>IMPORTANT</b> <i>This option appears only if Core node's ranges are not set as Device Under Test.</i></p> <p><i>See <a href="#">Paging Settings</a> for configuration details.</i></p>
<i>Trace Settings</i>	<i>Enable this option to send Trace Start/Deactivate Trace IEs as defined in TS38.413 chapter 8.11 (Trace Procedures). See <a href="#">Trace Settings</a> for configuration details.</i>
<i>Management Based MDT</i>	<i>Select to enable and click this setting to open the configuration panel. See <a href="#">Management Based MDT</a> for more details.</i>
<i>Mobile Terminated SMS Configuration</i>	<i>Select to enable and click this setting to open the configuration panel. See <a href="#">Mobile Terminated SMS Configuration</a> for more details.</i>
<i>Generic UE Configuration Update</i>	<i>Select to enable and click this setting to open the configuration panel.</i>

Setting	Description
Delay (s)	The time to wait, in seconds, before initiating the Generic UE Configuration Update procedure, after the UE is registered. A zero value means the procedure is not initiated.
Acknowledgment Request	If enabled (default), it indicates if the UE was asked to respond to the Configuration Update Command message with a <i>Configuration Update Complete</i> message.
Allocate New GUTI	If enabled (default), it will allocate a new Global Unique Temporary Identifier (GUTI) to the configuration update.

## Location Services

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

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

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

## NSSAI

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

Setting	Description								
<b>NSSAI:</b>									
	Select the <b>Add UE NSSAI</b> button to add a new UE NSSAI to your test configuration.								
<b>NSSAI Settings:</b>									
	Select the <b>Delete UE NSSAI</b> 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" data-bbox="344 1586 1437 1828"> <thead> <tr> <th data-bbox="344 1586 817 1638">SST</th> <th data-bbox="817 1586 1437 1638">Value</th> </tr> </thead> <tbody> <tr> <td data-bbox="344 1638 817 1691">eMBB</td><td data-bbox="817 1638 1437 1691">1</td></tr> <tr> <td data-bbox="344 1691 817 1744">URLCC</td><td data-bbox="817 1691 1437 1744">2</td></tr> <tr> <td data-bbox="344 1744 817 1828">MIoT</td><td data-bbox="817 1744 1437 1828">3</td></tr> </tbody> </table>	SST	Value	eMBB	1	URLCC	2	MIoT	3
SST	Value								
eMBB	1								
URLCC	2								
MIoT	3								

Setting	Description
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the S-NSSAI.
Mapped SST	The Mapped configured Slice/Service Type (SST) value for this S-NSSAI.
Mapped SD	The Mapped configured Slice Differentiator (SD) value for this S-NSSAI.

## Network Initiated PDU Session Modification

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

Setting	Description
<i>Network Initiated PDU Session Modification:</i>	
	From the panel, you can select a <b>DNN Config</b> for editing and also add additional DNN configurations. Select the <b>Add DNNs Config</b> button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the <b>Delete DNN Config</b> button to delete this DNN config from your test configuration.
DNN	From the drop-down, select one of the previously-defined DNNs.
Delay Before Network Initiated PDU Session Modification (s)	The time to wait, in seconds, between the PDU Session Establishment end and the start of Network Initiated PDU Session Modification procedure start.
Interval Between Consecutive Network Initiated PDU Session Modification procedures (s)	The time, in seconds, between two Consecutive Network Initiated PDU Session Modification procedures.
Iterations	The number of consecutive Network Initiated PDU Session Modification procedures per UE.
Flows:	<i>This option lists all the flows defined and associated to the selected DNN. Select the check-box to configure a flow. By default, the default bearer is selected.</i>

<b>Setting</b>	<b>Description</b>						
	Select the <b>Add Flow</b> button to add a new flow to your test configuration.						
<i>Flow:</i>							
	Select the <b>Delete Flow</b> button to delete this DNN config from your test configuration.						
Flow ID	Select the flow's ID from the drop-down list.						
ARP	<p><i>If enabled, the Allocation and Retention Priority (ARP) setting specifies the priority level, preemption capability, and preemption vulnerability of a resource request.</i></p>						
ARP Priority Level	<p>Specify the ARP priority level. The ARP Priority Level defines the relative importance of a resource request, where 1 is the highest priority and 15 is the lowest priority. The ARP priority levels 1–8 should be assigned only to resources for services that are authorized to receive prioritized treatment within an operator domain, whereas the ARP priority levels 9–15 may be assigned to resources that are authorized by home network and thus applicable when a UE is roaming.</p>						
ARP Preemption Capability	<p>The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Not Preempt</b></li> <li>• <b>May Preempt</b> - if selected, the packets in this Flow can preempt other flows. When a flow is preemption-capable, it can be allocated resources that were already assigned to another data flow that has a lower ARP priority level.</li> </ul>						
ARP Preemption Vulnerability	<p>The available options are:</p> <ul style="list-style-type: none"> <li>• <b>Not Preemptable</b></li> <li>• <b>Premptable</b> - if selected, 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.</li> </ul>						
GBR	<p><i>If enabled, configure the parameters to indicate the guaranteed bit rates (GBR) for the selected flow.</i></p>						
GBR Type	<p>Select the desired guaranteed bit rate (GBR) type for the flow. Based on your selection, LoadCore will show the appropriate settings to configure.</p> <table border="1" data-bbox="396 1670 1442 1873"> <tr> <td colspan="2" data-bbox="396 1670 1442 1748"> <i>QoS Rates:</i> </td></tr> <tr> <th data-bbox="396 1748 649 1805">Parameter</th><th data-bbox="649 1748 1442 1805">Description</th></tr> <tr> <td data-bbox="396 1805 649 1873">Uplink</td><td data-bbox="649 1805 1442 1873">Set the uplink bitrate.</td></tr> </table>	<i>QoS Rates:</i>		Parameter	Description	Uplink	Set the uplink bitrate.
<i>QoS Rates:</i>							
Parameter	Description						
Uplink	Set the uplink bitrate.						

<b>Setting</b>	<b>Description</b>																				
	<table border="1"> <tr> <td>Downlink</td><td>Set the downlink bitrate.</td></tr> <tr> <td colspan="2"><i>Dynamic QoS Rates:</i></td></tr> <tr> <th><b>Parameter</b></th><th><b>Description</b></th></tr> <tr> <td>Uplink Action</td><td>Select the action type to apply to the uplink bitrate.</td></tr> <tr> <td>Uplink Step</td><td>Select the step to increase or decrease the uplink bitrate.</td></tr> <tr> <td>Downlink Action</td><td>Select the action type to apply to the downlink bitrate.</td></tr> <tr> <td>Downlink Step</td><td>Select the step to increase or decrease the downlink bitrate.</td></tr> </table>	Downlink	Set the downlink bitrate.	<i>Dynamic QoS Rates:</i>		<b>Parameter</b>	<b>Description</b>	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.						
Downlink	Set the downlink bitrate.																				
<i>Dynamic QoS Rates:</i>																					
<b>Parameter</b>	<b>Description</b>																				
Uplink Action	Select the action type to apply to the uplink bitrate.																				
Uplink Step	Select the step to increase or decrease the uplink bitrate.																				
Downlink Action	Select the action type to apply to the downlink bitrate.																				
Downlink Step	Select the step to increase or decrease the downlink bitrate.																				
<i>MBR</i>	<i>If enabled, configure the maximum bit rates (MBR) allowed for the selected flos.</i>																				
MBR Type	<p>Select the desired maximum bit rate (MBR) type for the flow. Based on your selection, LoadCore will show the appropriate settings to configure.</p> <table border="1"> <tr> <td colspan="2"><i>QoS Rates:</i></td></tr> <tr> <th><b>Parameter</b></th><th><b>Description</b></th></tr> <tr> <td>Uplink</td><td>Set the uplink bitrate.</td></tr> <tr> <td>Downlink</td><td>Set the downlink bitrate.</td></tr> <tr> <td colspan="2"><i>Dynamic QoS Rates:</i></td></tr> <tr> <th><b>Parameter</b></th><th><b>Description</b></th></tr> <tr> <td>Uplink Action</td><td>Select the action type to apply to the uplink bitrate.</td></tr> <tr> <td>Uplink Step</td><td>Select the step to increase or decrease the uplink bitrate.</td></tr> <tr> <td>Downlink Action</td><td>Select the action type to apply to the downlink bitrate.</td></tr> <tr> <td>Downlink Step</td><td>Select the step to increase or decrease the downlink bitrate.</td></tr> </table>	<i>QoS Rates:</i>		<b>Parameter</b>	<b>Description</b>	Uplink	Set the uplink bitrate.	Downlink	Set the downlink bitrate.	<i>Dynamic QoS Rates:</i>		<b>Parameter</b>	<b>Description</b>	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>																					
<b>Parameter</b>	<b>Description</b>																				
Uplink	Set the uplink bitrate.																				
Downlink	Set the downlink bitrate.																				
<i>Dynamic QoS Rates:</i>																					
<b>Parameter</b>	<b>Description</b>																				
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.																				

## Core Network Assistance Information For Inactive

<b>Setting</b>	<b>Description</b>
<i>Core Network Assistance Information For Inactive</i>	
UE Specific DRX	The UE Specific DRX value can be selected from the available options: <ul style="list-style-type: none"> <li>• <b>DRX32</b></li> <li>• <b>DRX64</b> (default value)</li> <li>• <b>DRX128</b></li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• <b>DRX256</b></li> <li>• <b>None</b> - if selected, this IE will not be included in the message</li> </ul>
Include MICO Mode Indication	Indicates if the UE is configured with MICO Mode by the AMF. If disabled, this IE will not be included in the message.
<i>Expected UE Behaviour</i>	
Expected Handover Interval	<p>The expected time interval between inter NG-RAN node handovers. When set to <b>None</b>, this IE will not be included in the message. Select a value from the drop-down:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)</li> <li>• <b>Sec15</b></li> <li>• <b>Sec30</b></li> <li>• <b>Sec60</b></li> <li>• <b>Sec90</b></li> <li>• <b>Sec120</b></li> <li>• <b>Sec180</b></li> <li>• <b>Long Time</b></li> </ul>
Expected UE Mobility	<p>Indicates whether the UE is expected to be stationary or mobiles. When set to <b>None</b>, this IE will not be included in the message. Select a value from the drop-down:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)</li> <li>• <b>Stationary</b></li> <li>• <b>Mobile</b></li> </ul>
<i>Expected UE Activity Behaviour</i>	
Expected Activity Period	The expected activity time in seconds. Any period longer than 180 seconds is represented by the value 181. When left empty, this IE will not be included in the message.
Expected Idle Period	The expected idle time in seconds. Any period longer than 180 seconds is represented by the value 181. When left empty, this IE will not be included in the message.
Source Of UE Activity Behaviour Information	<p>Indicates the source of the UE activity behavior. When set to 'None' this IE will not be included in the message.</p> <p>Select a value from the drop-down:</p> <ul style="list-style-type: none"> <li>• <b>None</b> (default)</li> <li>• <b>Subscription Information</b></li> <li>• <b>Statistics</b></li> </ul>

## Paging Settings

Setting	Description
<i>Individual UE Paging</i>	
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 miliseconds.
<i>UE Group Paging</i>	<i>If selected, a group of Idle UEs will be paged from their last parent based on the configured criteria. The configuration is applied per parent node.</i>
Group Paging Condition	Select from the drop-down the condition that needs to be met in order to trigger Paging: <ul style="list-style-type: none"> <li>• <b>Time To Wait</b> - is counted from the moment the first UE goes to idle or after one iteration completes (in case iterations is used). When this time elapses, all the UEs that are idle at that moment will be paged.</li> <li>• <b>Number Of UEs</b> - when the respective amount of UEs are in idle state, Paging will be triggered for all of them.</li> </ul>
Group Paging Value	This is the condition value. The maximum value should be the same as for the maximum value for UE Range count.
Group Paging Iterations	The number of times to repeat the condition.
Group Paging Rate	The number of UEs per second for which Paging is started. The value zero disables the rate, and Paging will be done as soon as possible.
<i>Paging Throttling</i>	
Throttling Criterion	Select the criterion on which two consecutive Paging messages triggered by the downlink traffic should be sent: <ul style="list-style-type: none"> <li>• Seconds</li> <li>• Packets</li> </ul>
Value	Assign a number of seconds to wait, or packets to skip until Paging is sent again. A value of 0 disables this option.

## Trace Settings

Setting	Description
Trace Activation Delay (s)	Time, in seconds, after the UE registers to send the Trace Activation. A value of zero means the Trace Activation is sent within the ICS Request message.

<b>Setting</b>	<b>Description</b>
Trace Deactivation Delay (s)	Time, in seconds, after the trace activation was sent for the CoreSim to deactivate the trace. A value of zero disables the trace deactivation.
Interfaces to Trace	Select from the drop-down the interfaces to trace.
Trace Depth	The expected time interval between inter NG-RAN node handovers.
Trace Collection Entity IP Address	The starting IP address.
<i>MDT Settings</i>	
MDT Activation	<p>Select the Minimization of Drive Test (MDT) type used as MDT activation trigger. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Immediate MDT Only</b> (default)</li> <li>• <b>Logged MDT Only</b></li> <li>• <b>Immediate MDT Only and Trace</b></li> </ul>
Scope	<p>Select the area scope of the MDT. You can choose from:</p> <ul style="list-style-type: none"> <li>• <b>Cell Based</b></li> <li>• <b>TA Based</b></li> <li>• <b>PLMN Wide</b> (default)</li> <li>• <b>TAI Based</b></li> </ul>
<i>Cell Defining the Area Scope for MDT</i>	<p><b>IMPORTANT</b> This option appears only if the <b>Scope</b> is set to <b>Cell Based</b>.</p> <p>See <a href="#">Cell Defining the Area for MDT Settings</a> table for more details.</p>
<i>TACs Defining the Area Scope for MDT</i>	<p><b>IMPORTANT</b> This option appears only if the <b>Scope</b> is set to <b>TA Based</b>.</p> <p>See <a href="#">TACs Defining the Area for MDT Settings</a> table for more details.</p>
<i>TAIs Defining the Area Scope for MDT</i>	<p><b>IMPORTANT</b> This option appears only if the <b>Scope</b> is set to <b>TA Based</b>.</p> <p>See <a href="#">TAIs Defining the Area for MDT Settings</a> table for more details.</p>
Mode	<p>Select the MDT mode you want to apply. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Immediate MDT</b> (default)</li> <li>• <b>Logged MDT</b></li> </ul>
<i>Immediate MDT Settings</i>	<p><b>IMPORTANT</b> This option appears only if <b>Mode</b> is set to <b>Immediate MDT</b>.</p> <p>See <a href="#">Immediate MDT Settings</a> table for more details.</p>

Setting	Description
Logged MDT Settings	<p><b>IMPORTANT</b> This option appears only if <b>Mode</b> is set to <b>Logged MDT</b>. See <a href="#">Logged MDT Settings table</a> for more details.</p>
Signaling Based MDT	Select and click this setting to open the configuration panel. See <a href="#">Signaling Based MDT</a> for more details.

### Cell Defining the Area for MDT Settings

Setting	Description
TACS:	
	Select the Add TACS button to add a new UE ID to your test configuration.
Cell:	
	Select the Delete Cell ID button to delete the UE ID from your test configuration.
PLMN MCC	The PLMN Mobile Country Code (MCC) used in the construction of the Cell ID.
PLMN MNC	The PLMN Mobile Network Code (MNC) used in the construction of the Cell ID.
Cell ID	The cell identifier of the UE.

### TACs Defining the Area for MDT Settings

Setting	Description
TACS:	
	<p>This represents the Tracking Area Code (TAC) for this eNodeB. Select the <b>Add TAC</b> 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 <b>Delete</b> button to remove the tracking area code from your configuration.

## TAIs Defining the Area for MDT Settings

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

## Immediate MDT Settings

Setting	Description
<i>Measurements</i>	
Logging M1 Event Triggered Measurements	If enabled, the UE logs the M1 measurements (RSRP/RSRQ) that are triggered by specific events.
DL Signal Quantities (M1)	<i>Select to enable and click to open the configuration panel.</i>
Reporting Trigger	Select the trigger for M1 measurement report. Options are: <ul style="list-style-type: none"> <li>• <b>Periodic</b></li> <li>• <b>A2 Event Triggered</b></li> <li>• <b>A2 Event Triggered Periodic</b></li> </ul>
Event Type	<p><b>IMPORTANT</b> This option appears only if the <b>Reporting Trigger</b> is set to <b>A2 Event Triggered</b> or <b>A2 Event Triggered Periodic</b>.</p> <p>Select a specific type of radio event configured for data collection during MDT operations. Options are:</p> <ul style="list-style-type: none"> <li>• <b>RSRP</b></li> <li>• <b>RSRQ</b></li> <li>• <b>SINR</b></li> </ul>

Setting	Description
Event Threshold	<p><b>IMPORTANT</b> This option appears only if the <b>Reporting Trigger</b> is set to <b>A2 Event Triggered</b> or <b>A2 Event Triggered Periodic</b>.</p> <p>Set the value for the event. Allowed values are between 0 (default) and 127.</p>
Report Interval	<p><b>IMPORTANT</b> This option appears only if the <b>Reporting Trigger</b> is set to <b>Periodic</b> or <b>A2 Event Triggered Periodic</b>.</p> <p>Select from the drop-down the time interval between successive event notifications. Possible values are: <b>ms120</b>, <b>ms240</b>, <b>ms480</b>, <b>ms640</b>, <b>ms1024</b>, <b>ms2048</b>, <b>ms5120</b>, <b>ms10240</b>, <b>min1</b>, <b>min6</b>, <b>min12</b>, <b>min30</b>, <b>min60</b>.</p>
Report Amount	<p><b>IMPORTANT</b> This option appears only if the <b>Reporting Trigger</b> is set to <b>Periodic</b> or <b>A2 Event Triggered Periodic</b>.</p> <p>Select from the drop-down the number of measurement reports that the UE sends to the network before stopping. Possible values are: <b>r1</b>, <b>r2</b>, <b>r4</b>, <b>r8</b>, <b>r16</b>, <b>r32</b>, <b>r64</b>, <b>infinity</b>.</p>
<i>Power Headroom (M2)</i>	<i>Select to enable and click to open the configuration panel.</i>
<b>Enable M2 Measurement</b>	If enabled, the UE will transmit Power Headroom (M2) values measured as the difference between the maximum transmission power of the UE and the current transmission power that the UE is using.
<i>PDCP SDU Data Volume (M4)</i>	<i>Select to enable and click to open the configuration panel.</i>
<b>Collection Period</b>	Select the time duration over which the User Equipment (UE) collects measurement data related to network performance. Possible values are: <b>ms1024</b> , <b>ms2048</b> , <b>ms5120</b> , <b>ms10240</b> , <b>min1</b> .
<b>Links to log</b>	Specifies which direction of the communication channel the measurements are collected from, impacting how network performance is analyzed and optimized. Available options are: <ul style="list-style-type: none"> <li>• <b>Uplink</b></li> <li>• <b>Downlink</b></li> <li>• <b>Both Uplink and Downlink</b></li> </ul>
<i>Average UE Throughput (M5)</i>	<i>Select to enable and click to open the configuration panel.</i>
<b>Collection Period</b>	Select the time duration over which the User Equipment (UE) collects measurement data related to network performance. Possible values

Setting	Description
	are: <b>ms1024</b> , <b>ms2048</b> , <b>ms5120</b> , <b>ms10240</b> , <b>min1</b> .
Links to log	Specifies which direction of the communication channel the measurements are collected from, impacting how network performance is analyzed and optimized. Available options are: <ul style="list-style-type: none"> <li>• <b>Uplink</b></li> <li>• <b>Downlink</b></li> <li>• <b>Both Uplink and Downlink</b></li> </ul>
<i>Packet Delay (M6)</i>	<i>Select to enable and click to open the configuration panel.</i>
Report Interval	Select from the drop-down the time interval between successive event notifications. Possible values are: <b>ms120</b> , <b>ms240</b> , <b>ms480</b> , <b>ms640</b> , <b>ms1024</b> , <b>ms2048</b> , <b>ms5120</b> , <b>ms10240</b> , <b>ms20480</b> , <b>ms40960</b> , <b>min1</b> , <b>min6</b> , <b>min12</b> , <b>min30</b> .
Links to log	Specifies which direction of the communication channel the measurements are collected from, impacting how network performance is analyzed and optimized. Available options are: <ul style="list-style-type: none"> <li>• <b>Uplink</b></li> <li>• <b>Downlink</b></li> <li>• <b>Both Uplink and Downlink</b></li> </ul>
<i>Packet Loss Rate (M7)</i>	<i>Select to enable and click to open the configuration panel.</i>
Collection Period	Set the period (in minutes) in which the collection of data will occur.
Links to log	Specifies which direction of the communication channel the measurements are collected from, impacting how network performance is analyzed and optimized. Available options are: <ul style="list-style-type: none"> <li>• <b>Uplink</b></li> <li>• <b>Downlink</b></li> <li>• <b>Both Uplink and Downlink</b></li> </ul>

## Logged MDT Settings

Setting	Description
Report Type	Select the report type for logged MDTs. Options are: <ul style="list-style-type: none"> <li>• <b>Periodic</b></li> <li>• <b>Event Triggered</b></li> </ul>
Logging Interval	Specifies the time interval between consecutive logged measurements. Possible values are: <b>ms320</b> , <b>ms640</b> , <b>ms1280</b> , <b>ms2560</b> , <b>ms5120</b> ,

Setting	Description
	<b>ms10240, ms20480, ms30720, ms40960, ms61440, infinity.</b>
Logging Duration	Defines the total duration for which the UE should perform logging of measurements. Once this duration expires, the UE stops logging. Possible values are: <b>m10, m20, m40, m60, m90, m120.</b>
Event Trigger	<p><b>IMPORTANT</b> This option is available only if the <b>Report Type</b> is set to <b>Event Triggered</b>.</p> <p>Select from the drop-down the type of event trigger. Options are:</p> <ul style="list-style-type: none"> <li>• <b>Out of Coverage</b></li> <li>• <b>L1 Event</b></li> </ul>
L1 Event Type	<p><b>IMPORTANT</b> This option is available only if the <b>Event Trigger</b> is set to <b>L1 Event</b>.</p> <p>Select the threshold type of the L1 event trigger:</p> <ul style="list-style-type: none"> <li>• <b>RSRP</b></li> <li>• <b>RSRQ</b></li> </ul>
L1 Event Threshold	<p><b>IMPORTANT</b> This option is available only if the <b>Event Trigger</b> is set to <b>L1 Event</b>.</p> <p>Specify the threshold value for triggering a Layer 1 event.</p>
Hysteresis	<p><b>IMPORTANT</b> This option is available only if the <b>Event Trigger</b> is set to <b>L1 Event</b>.</p> <p>Define a margin above or below the L1 Event Threshold that must be exceeded before the event is triggered or canceled.</p>
Time to Trigger	<p><b>IMPORTANT</b> This option is available only if the <b>Event Trigger</b> is set to <b>L1 Event</b>.</p> <p>Select from the drop-down the time during which specific criteria for the event has to be met in order to trigger a measurement report. Available values are: <b>ms0, ms40, ms64, ms80, ms100, ms128, ms160, ms256, ms320, ms480, ms512, ms640, ms1024, ms1280, ms2560, ms5120.</b></p>

## Signaling Based MDT

Setting	Description
PLMNs:	
	Select the Add PLMN button to add a new public land mobile network to your test configuration.
PLMN:	

<b>Setting</b>	<b>Description</b>
	Select the Delete PLMN button to delete the public land mobile network from your test configuration.
PLMN MCC	The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.
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. Add the MNC that will be assigned to each UE in this range.

### Management Based MDT

<b>Setting</b>	<b>Description</b>
<i>PLMNs:</i>	
	Select the Add PLMN button to add a new public land mobile network to your test configuration.
<i>PLMN:</i>	
	Select the Delete PLMN button to delete the public land mobile network from your test configuration.
PLMN MCC	The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.
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. Add the MNC that will be assigned to each UE in this range.

### Mobile Terminated SMS Configuration

<b>Setting</b>	<b>Description</b>
Delay	After the UE registers, the network waits the configured number of seconds before it initiates the MT SMS.
Originating Address	The originating address of the SMS text message.
Service Center Address	The service center address of the SMS text message.
Type of Number	Select from the drop-down the type of number to be used. Options are: <ul style="list-style-type: none"> <li>• Unknown</li> <li>• International Number</li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• National Number</li> <li>• Network Specific Number</li> <li>• Subscriber Number</li> <li>• Alphanumeric</li> <li>• Abbreviated Number</li> <li>• Reserved Number</li> </ul>
Numbering Plan Identification	Select from the drop-down the numbering plan identification. Options are: <ul style="list-style-type: none"> <li>• Unknown</li> <li>• ISDN</li> <li>• Data Numbering Plan</li> <li>• Telex Numbering Plan</li> <li>• National Numbering Plan</li> <li>• Private Numbering Plan</li> <li>• Ermes Numbering Plan</li> <li>• Reserved Numbering Plan</li> </ul>
Text	The actual text message of the SMS.
Character Set	Select the character set used in the data coding scheme for the text message. Options are: <ul style="list-style-type: none"> <li>• GSM7</li> <li>• UCS2</li> </ul>

## 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**.

<b>Setting</b>	<b>Description</b>									
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"> <thead> <tr> <th><b>Scheme</b></th> <th><b>Identifier</b></th> <th><b>Size of the scheme output</b></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> </tbody> </table>	<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>	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
<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>								
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								

<b>Setting</b>	<b>Description</b>		
	<b>Scheme</b>	<b>Identifier</b>	<b>Size of the scheme output</b>
	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, <b>5G-AKA</b> 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"> <li>• <b>64 kbps</b></li> <li>• <b>Full Data Rate</b></li> </ul>		
Integrity Protection Maximum Downlink Data Rate	<p>Select a value from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>64 kbps</b></li> <li>• <b>Full Data Rate</b></li> </ul>		

Setting	Description
<i>UDM User Plane Security Profile</i>	<i>With this option you can configure User Plane security profiles. See <a href="#">UDM User Plane Security Profile below</a> table for details.</i>
<i>Override UE Security Capability</i>	<i>If selected, this option will override the default UE Security Capability settings. See <a href="#">Override UE Security Capability on the facing page</a> table for details.</i>

## UDM User Plane Security Profile

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

Parameter	Description
	Select the <b>Add Security Profile</b> button to add a new profile to your test configuration.
	Select the <b>Delete Profile</b> 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"> <li>• <b>REQUIRED</b></li> <li>• <b>PREFERRED</b></li> <li>• <b>NOT-NEEDED</b></li> </ul>
Confidentiality	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>REQUIRED</b></li> <li>• <b>PREFERRED</b></li> <li>• <b>NOT-NEEDED</b></li> </ul>

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.

## Override UE Security Capability

The following parameters are required to configure the Override UE Security Capability:

Parameter	Description
Include 5G UE Security Capabilities in 4G Attach	If enabled, the 4G Attach Request will contain the UE Additional Security Capability IE (5G UE Security Capability).
<i>5G Ciphering Algorithm</i>	<i>This section lists the supported 5G ciphering algorithm. By default, all settings are enabled. If required, you can disable each setting individually to avoid override.</i>
NEA0	Null ciphering algorithm (enabled by default).
NEA1	128-bit SNOW 3G based algorithm (enabled by default).
NEA2	128-bit AES based algorithm (enabled by default).
NEA3	128-bit ZUC based algorithm (enabled by default).
<i>5G Integrity Algorithm</i>	<i>This section lists the supported 5G integrity algorithm. By default, all settings are enabled. If required, you can disable each setting individually to avoid override.</i>
NIA0	Null ciphering algorithm (enabled by default).
NIA1	128-bit SNOW 3G based algorithm (enabled by default).
NIA2	128-bit AES based algorithm (enabled by default).
NIA3	128-bit ZUC based algorithm (enabled by default).

## UE Subscribed AMBR settings

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

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

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

## DNNs Config

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

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

Setting	Description
<i>DNNs Config:</i>	
	From the panel, you can select a DNN Config for editing and also add additional DNN configurations. Select the <b>Add DNNs Config</b> button to add a new DNN configuration.
<i>DNN Config:</i>	
	Select the <b>Delete DNN Config</b> 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"> <li>SSC Mode 1: The network preserves the connectivity service provided to the UE. The PDU Session IP address (IPv4, IPv6, IPv4v6) is preserved.</li> <li>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.</li> <li>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.</li> </ul>
Session ID	Provide the session ID value.
DNN	Select one of the previously-defined DNNs from the drop-down list.
Local IPv4 Address	<p>The IPv4 address that the UE receives from the SMF during PDU Session Establishment. This address is used for L4-7 traffic (source IP for the UL traffic, destination IP for the DL traffic). It is used only when LoadCoresimulates the SMF.</p> <p>IP address is also used to create UE Routes from DN.</p>

<b>Setting</b>	<b>Description</b>
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:	<p><i>When this check-box is selected, you can configure which slice (S-NSSAI) to be send in PDU Session Establishment messages. If the check-box is not selected, the first slice from Allowed NSSAI list (received in Registration Accept) is used in PDU Session Establishment message.</i></p> <div style="border: 1px solid #ccc; padding: 5px; margin-left: 10px;"> <b>NOTE</b> <i>This is applicable for the N1/N2 interface only and is not propagated beyond the AMF.</i> </div>
S-NSSAI	This list contains all the slices defined for the selected UE range. Select from the drop-down list the slice to be used in PDU Session Establishment.
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"> <li>• 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).</li> <li>• 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.</li> </ul> <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"> <li>• <b>None</b></li> <li>• <b>EAP-TTLS</b> (Extensible Authentication Protocol – Tunnelled Transport Layer Security)</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>• <b>CHAP</b> (Challenge-Handshake Authentication Protocol)</li> <li>• <b>PAP</b> (password Authentication Protocol)</li> </ul>
<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"> <li>• <b>PAP</b></li> <li>• <b>CHAP</b></li> </ul>
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.

## 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"> <li>• Unknown</li> <li>• International number</li> <li>• National number</li> <li>• Network specific number</li> <li>• Subscriber number</li> <li>• Alphanumeric</li> <li>• Abbreviated number</li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• Reserved number</li> </ul>
Numbering Plan Identification	<p>The numbering plan identification can be one of the following:</p> <ul style="list-style-type: none"> <li>• Unknown</li> <li>• ISDN</li> <li>• Data numbering plan</li> <li>• Telex numbering plan</li> <li>• National numbering plan</li> <li>• Private numbering plan</li> <li>• ERMES numbering plan</li> <li>• Reserved numbering plan</li> </ul>
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>SMSF Configuration:</i>	
SMS Mode	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>SMS-MO:</b> Mobile Originated. The UE range originates (sends) SMS messages.</li> <li>• <b>SMS-MT:</b> Mobile Termintated. The UE range waits for delivery of SMS messages.</li> </ul>

## Untrusted WiFi Settings

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

<b>Setting</b>	<b>Description</b>
Remote N3IWF	Select the remote N3IWF range from drop-down list.
Destination Port	Read-only field. Value set to <b>500</b> .
Source Port	Provide the source port. By default, set to <b>500</b> .
Enable NAT-T	Select to enable the NAT Traversal keepalive.
NAS IP Type	Select the NAS IP type from the drop-down list: <b>IPv4</b> (default) or <b>IPv6</b> .
Configure a CA Certificate	<p>By default this option is disabled.</p> <p>When enabled, the CA Certificate drop-down is displayed which allows the</p>

<b>Setting</b>	<b>Description</b>
	selection of one of the CA Certificates defined in <a href="#">global settings</a> .
CA Certificate	Select the CA Certificate from the drop-down list.
<i>IKE Phase 1</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: <b>AES-128-GCM-16</b> . Available options are: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b> .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: <b>NONE</b> . Available options: <b>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</b> . Restrictions: <ul style="list-style-type: none"> <li>• When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>• If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
DH Group	Select an option from the drop-down list. Available options are: <b>modp768(1), modp1024(2), modp1536(5), modp2048(14), modp3072(15), modp4096(16), modp6144(17), modp8192(18), prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32)</b> . Default value: <b>prime256v1(19)</b> .
PRF Algorithm	Select an option from the drop-down list. Default value: <b>HMAC-SHA256</b> . Available options: <b>HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512</b> .
<i>IKE Phase 2</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: <b>AES-128-GCM-16</b> . Available options: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b> .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: <b>NONE</b> . Available options: <b>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</b> .

Setting	Description
	<p>Restrictions:</p> <ul style="list-style-type: none"> <li>When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list. Available options are: <b>ID_IPV4_ADDR</b>, <b>ID_FQDN</b>, <b>ID_USER_FQDN</b>, <b>ID_IPV6_ADDR</b>, <b>ID_DER ASN1 DN</b>, <b>ID_KEY_ID</b>.</p> <p>Default value: <b>ID_FQDN</b>.</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: <b>ID_FQDN</b>, <b>ID_KEY_ID</b> or <b>ID_RFC822_ADDR</b>.</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: <b>0</b> (disabled).</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>
DPD Interval (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>

## 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** ..... **1068**

**UDM SNSSAI Mappings** ..... **1069**

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

## Objectives

In a 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** ..... **1069**

**User Plane Objectives** ..... **1082**

### 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>	$20000 / 1000 = 20\text{s}$ 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"> <li><b>Active Subscribers:</b> 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.</li> <li><b>Subscribers Per Second:</b> The test attempts to activate a specified number of subscriber sessions per second, within the rate and time parameters that you configure.</li> </ul> <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 <b>DNNs Config</b> Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> <li>All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> <p>The list of available DNNs include those that have not been activated for the primary objective.</p>
Number of	This value indicates how many times UE/NGRAN will retry the Register or PDU

Parameter	Description
Retries	<p>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"> <li>• <b>-1</b> : infinite retries for entire sustain time.</li> <li>• <b>0</b> (default value) : the retry option is disabled.</li> <li>• <b>1 to 127</b>: the number of retries per UE (Register + PDU Session procedure).</li> </ul>
<i>Subscribers Per Second:</i>	
Hold Time (s)	The number of seconds that each subscriber session will remain active. This is, therefore, the amount of time that will elapse between the subscriber attach and the subscriber detach. At the end of the session hold time, the subscriber performs the detach procedure.
Rate	The number of subscriber sessions to activate per second.
Sustain Time (s)	The duration of time (in Seconds) that the specified session activation rate will be maintained.
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the objective after NG-Setup/S1-Setup have successfully completed.
DNNs to Activate	<p>Select the DNNs to activate for this secondary objective. (These are the DNNs configured for the UE in the <b>DNNs Config</b> Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> <p>The list of available DNNs include those that have not been activated for the primary objective.</p>

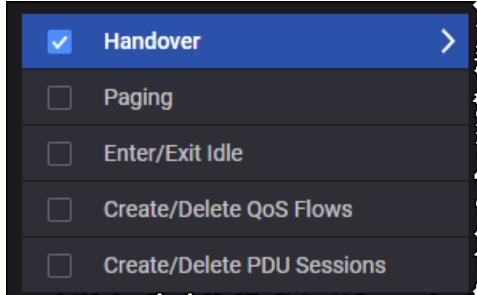
## Secondary Control Plane Objective

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:

<b>When the primary objective is:</b>	<b>then the secondary objectives will start...</b>
Active Subscribers	after all users are registered.
Subscribers Per Second	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).

### 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 <b>Distributed over (s)</b> 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.

Parameter	Description
Max Outstanding	The maximum number of UE registration procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Force N2 Handover	Enable this option to force N2 handover with direct forwarding instead of X2 / Xn handover.
Mobility for State	<p>This option specifies in what state should the UE perform the handover objective. The following options can be selected from the drop-down list:</p> <ul style="list-style-type: none"> <li>• <b>Connected</b></li> <li>• <b>Idle</b></li> <li>• <b>Any</b></li> </ul> <p>When <b>Any</b> 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"> <li>• <b>None</b> - 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.</li> <li>• <b>Connected</b> - The UE will perform Connected Handover from the last node in the visited gNodeBs/eNodeBs list to the parent RAN. This means that <b>if the UE was in idle state</b> before performing this mobility, the UE will <b>first perform exit idle</b>, and only after the UE is in connected state, will it initiate <b>the connected handover</b> to the parent RAN.</li> <li>• <b>Idle</b> - 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 <b>connected</b> state before performing this mobility, the UE will <b>first perform enter idle</b>, and only after the UE is in idle state, will it initiate the <b>idle mode mobility</b> to the parent RAN.</li> </ul>
Send Service Request after Returning to Parent Node	<p>By default, this option is disabled.</p> <p>Send Service Request immediately after Return to Parent Node Mobility if UE State was idle.</p>
Handover Cancel	<i>When this option is enabled, NG-RAN will trigger a Handover Cancel after receiving Handover Request from AMF. Handover Cancel is applicable only for N2 Handover.</i>
Percentage	The percentage of N2 Handover Procedures that will trigger a Handover Cancel from the gNodeB.

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

## Paging

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

The following table describes the Paging objective parameters.

Parameter	Description
<i>Paging:</i>	
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max	The maximum number of procedures that may be outstanding while new

Parameter	Description
Outstanding	procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay (s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
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"> <li>If the UPF is the DUT in the test topology, then set the <i>Remote IP Address</i> to the DN IP address.</li> <li>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.</li> </ul>

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	Used to configure procedure rate less than 1/sec. Example: if configured as 3,

Parameter	Description
Over (s)	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

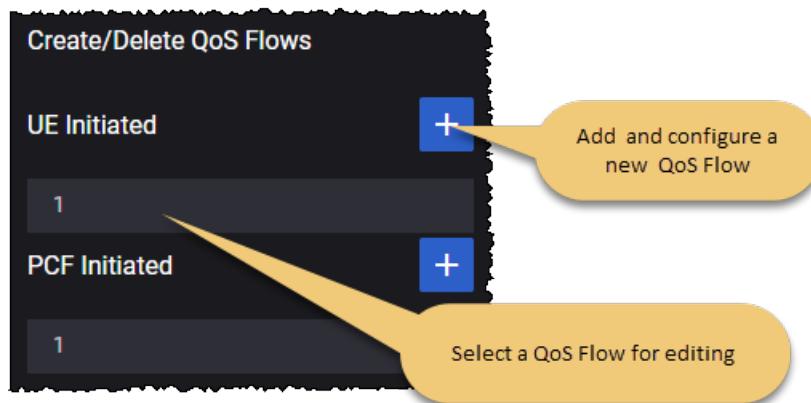
When you configure a **Create/Delete QoS Flows** secondary objective, each of the active subscribers configured for the primary objective attempts to meet the requirements defined by the QoS Flow ID. The selected flows will be created following a configured *Delay* value, and deleted when the configured *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 <b>Add Objective</b> button to add an instance of this objective.
<i>Objective:</i>	
	Select the <b>Delete Objective</b> button to delete this Secondary Objective from your test configuration.
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	The rate at which procedures are initiated, measured in procedures initiated per second. Using higher values for this parameters requires a large number of UEs configured in the test in order to achieve the desired rate.
Distributed over (s)	Used to configure procedure rate less than 1/sec. Example: if configured as 3, test will execute one procedure every 3 seconds.
Max Outstanding	The maximum number of procedures that may be outstanding while new procedures are being started. If the number of outstanding procedures reaches this limit, no new procedures may be started until the outstanding procedures have successfully started.
Delay(s)	The number of seconds to wait before starting the secondary objective, from the start of sustain time.
Interval	Interval between the triggering of creation and deletion of the QoS flow, in seconds.
DNN	Select the DNN value for the drop-down list. For example: 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 <b>Add Objective</b> button to add an instance of this objective.
<i>Objective:</i>	
	Select the <b>Delete Objective</b> 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

Parameter	Description
	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 <b>DNNs Config</b> Range settings.)</p> <p>The choices are:</p> <ul style="list-style-type: none"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> <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 <b>DNNs Config</b> 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.

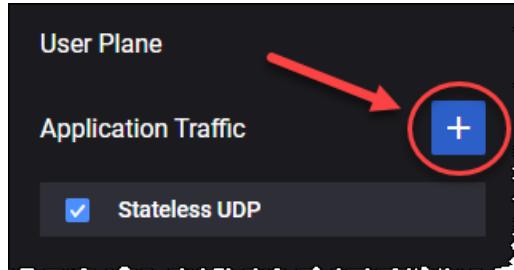
Parameter	Description
Iterations	The number of times this procedure runs for each subscriber, it can be finite or infinite (set to zero).
Rate	<p>The rate at which procedures are initiated, measured in procedures initiated per second.</p> <p>Using higher values for this parameter requires a large number 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.

Parameter	Description
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, Ping, Synthetic and UDG**.

**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"><li>• <b>Stateless UDP</b></li><li>• <b>Data</b></li><li>• <b>Voice</b></li><li>• <b>Video OTT</b></li><li>• <b>DNS Client</b></li><li>• <b>Predefined Applications</b></li><li>• <b>ICMP Client</b></li><li>• <b>Capture Replay</b></li><li>• <b>Synthetic</b></li></ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>• <b>UDG</b></li> </ul>
	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 <a href="#">Stateless UDP Traffic</a> .
Data	For the settings required to configure the Data traffic objective, refer to <a href="#">Data Traffic</a> .
Voice	For the settings required to configure the Voice traffic objective, refer to <a href="#">Voice Traffic</a> .
Video OTT	For the settings required to configure the Video OTT traffic objective, refer to <a href="#">Video Ott Traffic</a> .
DNS Client	For the settings required to configure the DNS Client objective, refer to <a href="#">DNS Client Traffic</a> .
Predefined Applications	For the settings required to configure the Predefined Applications objective, refer to <a href="#">Predefined Applications Traffic</a> .
Synthetic	For the settings required to configure the Synthetic traffic objective, refer to <a href="#">Synthetic Traffic</a> .
UDG	For the settings required to configure the UDG traffic objective, refer to <a href="#">UDG Traffic</a> .
REST API Client	For the settings required to configure the REST API Client objective, refer to <a href="#">REST API Client</a> .

## 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 <b>Stateless UDP</b> .
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 <b>uplink</b> 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

Parameter	Description
	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 <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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 <b>Data</b> .
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 <b>Throughput</b> . The other options are: <b>Concurrent Connections</b> and <b>Connections Rate</b> .
Concurrent Connections	Set the number of concurrent connections. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connection Duration (s)	Set a value for the connection duration. This parameter is available only when Objective type is set to <b>Concurrent Connections</b> .
Connections Rate per Second	Set the value for connections rate per second. This parameter is available only when Objective type is set to <b>Connections Rate</b> .
Throughput (kbps)	The desired throughput (in kbps) for the combined traffic flows that will be generated.
Optimize Throughput (per UE)	Select this option to enable it.
Connection Multiplier (per UE)	Set the connection multiplier value.
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.  The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Delay application traffic start (ms)	The time (in milliseconds) to wait before the application traffic flows start after each PDU Session has been established.
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .

Parameter	Description
Application Traffic Flows	<p>Each Application Traffic entry requires at least one traffic flow definition, and can support multiple such definitions.</p> <ul style="list-style-type: none"><li>• To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li><li>• To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li></ul> <p>Refer to <a href="#">Flow</a> for a description of the configuration settings for these traffic flows. Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Flow</b> 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"> <li>If <a href="#">Optimize Throughput (per UE)</a> option is enabled: <b>TCP</b>, <b>TLS</b>, <b>QUIC</b> or <b>UDP</b>.</li> <li>If <a href="#">Optimize Throughput (per UE)</a> option is disabled: <b>TCP</b>, <b>TLS</b> or <b>UDP</b>.</li> </ul>
Type	Select the L4/L7 protocol type from the list of pre-defined flows. The available options are: <ul style="list-style-type: none"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get</b>, <b>HTTP Put</b>, <b>HTTP Post</b> and <b>FTP</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get</b>, <b>HTTPS Put</b> and <b>HTTPS Post</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Get</b>, <b>HTTP3 Put</b> and <b>HTTP3 Post</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional</b> (a flow in which a UDP client communicates with a server over a bidirectional datagram socket)</li> </ul> <p><b>NOTE</b> UDP bidirectional works for each UE by sending the number of TX packets configured in the objective (by default 8). After the packets have been received by the DN (or UPF), it sends RX packets (by default 8) to each UE. If the UEs receives the packets, they will send again the number of TX packets and so on. If the UEs did not receive downlink packets, it will send another set of TX packets after 60 seconds.</p>
Port	The port used by the flow.
Iterations	The number of times the flow will run. It can be finite or infinite (set to zero). For example, a flow may have default actions: log in to a social media site, post a message, then log out. Iterations is the number of times you want this flow of actions to be executed.
Percentage	The percentage of the throughput will be of this type of flow.
Page Size (bytes)	The page size represents the size of the web page or data file that will be retrieved from or stored to an HTTP or FTP server.
Client Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> for more details.
Server Tx Count	This parameter is available only when the flow type is set to UDP Bidirectional. Refer to <a href="#">UDP Bidirectional</a> 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.
QoS FlowID	Select a QoS Flow ID for this flow.

## Custom Parameters

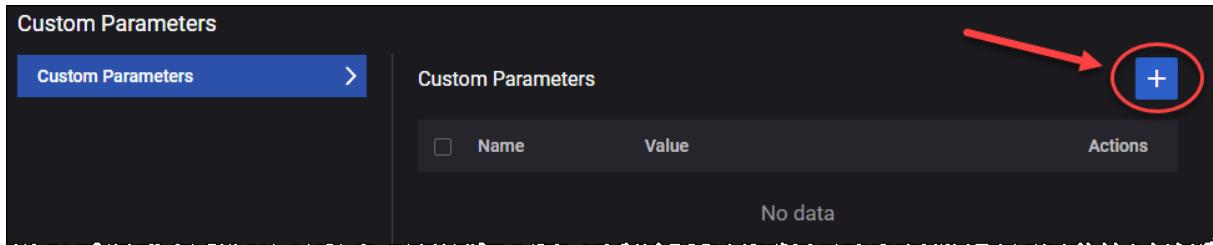
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

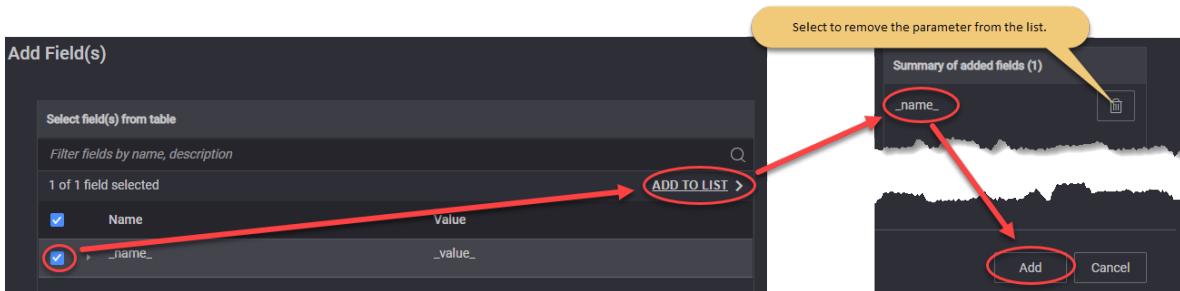
2. Select the **Add** button.



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 <b>Voice</b> .
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 <b>Simulated Users</b> 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: <b>IPv4</b> or <b>IPv6</b> .
Call Type	<p>Select the type of call from the drop-down list. Available options are:</p> <ul style="list-style-type: none"> <li>• <b>Basic Call</b></li> <li>• <b>Basic Call Mo</b> (Mobile Originated)</li> <li>• <b>Basic Call Mt</b> (Mobile Terminated)</li> <li>• <b>Custom Flow</b></li> </ul> <p>When creating a new test or when adding a new UE range, the Call Type default option is the <b>Basic Call</b>, which allows you to run a basic SIP call without the IMS entity and with DN simulating the Mobile Terminating (MT) side.</p> <p>When selecting <b>Basic Call MO/Basic Call MT</b>, the app will use a predefined SIP Flow intended for the use-case in which a DUT IMS or simulated IMS is involved.</p> <p>If the test requirements need an extended set of SIP flows or higher level of flexibility, it is recommended to use the <b>Custom Flow</b> Call Type, which enables the Flow Editor.</p>
Flow Editor:	<p><b>IMPORTANT</b> This configurator becomes available only if Call Type is set to Custom Flow.</p>

Parameter	Description
	<i>Click to open the page and create a particular state machine for SIP calls that allows you a higher flexibility to customize the SIP message sequence and SIP headers/SDP body as desired. For settings, refer to <a href="#">Flow Editor</a> section.</i>
Dial Plan:	<i>For the settings required to configure the dial plan, refer to <a href="#">Dial Plan</a>.</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"> <li>• <b>TCP</b> - Transmission Control Protocol</li> <li>• <b>TLS</b> - Transport Layer Security</li> <li>• <b>UDP</b> - User Datagram Protocol</li> </ul>
Domain	Provide the domain name.
Persistent TCP Connection	If enabled, it will not close the TCP connection on the iteration end.
Enable IPSEC	Select this option to enable IPSEC.
Registration Refresh Time	Select whether to use a <b>Negotiated</b> refresh time, or a <b>Custom</b> type: <ul style="list-style-type: none"> <li>• <b>Negotiated</b> - the registration refresh will be sent after 50% of the expiration time received in <b>200 OK</b> response.</li> <li>• <b>Custom</b> - allows you to set the registration refresh interval</li> </ul>
Custom Registration Refresh Interval (s)	This parameter appears only if <b>Registration Refresh Time</b> is set to <b>Custom</b> . The time interval (in seconds) to send SIP Registration Refresh.
Number of Loops after Registration to Send Deregistration	This parameter will send the SIP Deregister at the end of each configured iteration number.
Advanced SIP Settings	For more details about these settings, refer to <a href="#">Advanced SIP Settings</a> .
<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.

Parameter	Description
Enable OWD	If selected, one way delay statistics for audio RTP traffic are computed.
Enable RTCP	Select this option in order to enable RTCP.
Enable SRTP	Select this option in order to enable Secure Real-time Transport Protocol (SRTP).
RTP Session Duration (ms)	Set the value for the session duration.
<i>Audio settings:</i>	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
<i>Video Settings:</i>	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
<i>MSRP Settings:</i>	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
<i>MCTTP Settings</i>	<i>For the configuration of MCTTP settings, refer to <a href="#">MCPTT Settings</a>.</i>
<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"> <li>• <b>None</b></li> <li>• <b>EVS/AMR IPv4</b></li> <li>• <b>NB Codecs IPv6</b></li> <li>• <b>AMR-WB IPv6</b></li> <li>• <b>Multimedia IPv4</b></li> </ul>
<i>QoE Settings</i>	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

## Flow Editor

Press  to open the editor's window. The following settings are available:

Parameter	Description
Procedures Library	<p><b>TIP</b> This library can also be accessed from Test Overview &gt; Procedures Library, while the procedures are managed from the <a href="#">Settings &gt; Resource Library</a>.</p> <p>Select to access the Procedures Library, where you will find the following categories:</p> <ul style="list-style-type: none"> <li>• <b>SIP</b> - will include the procedures related to SIP signaling.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li><b>Media</b> - will include the procedures related to media (audio or/and video)</li> <li><b>Flow</b> - will include the Start and Stop procedures used to define an iteration. The number of iterations can be configured per each UE range on the Voice objective, Dial Plan section (0 meaning infinite loops).</li> </ul> <p>See <a href="#">Procedures Library</a> for more information.</p>
Current Range	This field will be automatically populated with the name of the UE range on which the Voice application traffic is configured.
Add required procedures first > Procedures	Add the procedures required for this custom flow.
Linked Range	Select from the drop-down the UE range that will be connected. Then, add the procedures corresponding to the configuration of state machine.

Note that every procedure added under the Procedures list includes an **Add +** button and an **Expand** button:

- Use the Expand button to see the **Next On Success** and **Next on Error** configuration fields for the respective procedure. Proceed on setting up these fields for each procedure added.
- Use the **Add** button to add more steps to the procedure. Set the procedures as above.
- The red connections that appear between procedures will let you know how these are connected.

See also the [Procedures Resources \(SIP/Media/Flow\)](#) section for complete information on:

- [procedures resources and their management](#)
- [adding predefined procedures](#) from the Resource Library
- [using the Flow Editor](#) and other configurations required
- [creating a procedure from scratch](#)

## Dial Plan

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

Parameter	Description
DNN	Select the DNN from the drop-down list.
Destination IP	The destination IP address.
Destination IP Increment	The value by which the destination IP is incremented.
Iterations	The number of times the Call Type will be executed. It can be finite or infinite (set to zero).

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

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Video	Select the QoS flow used for audio from the drop-down list.
<i>Jitter Buffer Settings:</i>	
Initial Delay (ms)	Set the value of the initial delay until playback starts (ms).
<i>Audio Codecs</i>	
	Select this button to add the audio codec to your test configuration.
	Select this button to remove the audio codec from your test configuration.
Codec Name	Select the audio codec from the drop-down list. The available options are: <ul style="list-style-type: none"> <li><b>AMR</b> - 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.</li> <li><b>AMR-WB</b> - The Adaptive Multi-Rate Wide Band (AMR-WB) is an audio data</li> </ul>

Parameter	Description
	<p>compression schemes optimized for speech coding, which have been adopted as the standard speech codec by 3GPP.</p> <ul style="list-style-type: none"> <li>• <b>EVS</b> - 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.</li> <li>• <a href="#"><b>PCMU</b></a></li> <li>• <a href="#"><b>PCMA</b></a></li> <li>• <a href="#"><b>iLBC</b></a></li> <li>• <a href="#"><b>G722</b></a></li> <li>• <a href="#"><b>G723</b></a></li> <li>• <a href="#"><b>G729</b></a></li> </ul> <p>The parameters of each audio codec are presented below.</p>

## AMR/AMR-WB

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

## EVS

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet.
Payload Type	Specifies the audio payload type.
Payload Format	The following options are available: <ul style="list-style-type: none"> <li><b>Full header</b> - 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.</li> <li><b>Compact</b> - 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.</li> </ul>
Bitrate	Indicates the mode(bitrate) of the EVS codec. Select the value from the drop-down list.

### PCMU/PCMA/iLBC/G722/G723/G729

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

### Video Settings

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

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

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

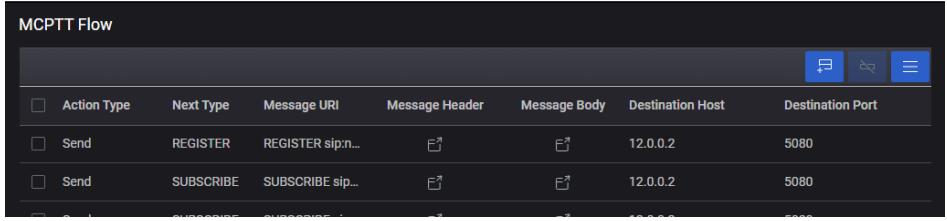
## MSRP Settings

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

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

## MCPTT Settings

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

Parameter	Description																					
Enable MCPTT	Select to enable this option.																					
QoS Flow ID for MCPTT	Select the QoS Flows ID(s) from the drop-down list.																					
MCPTT Message Format	The MCPTT message format defined according to TS 24.380 standard.																					
MCPTT Group	The first MCPTT Group ID.																					
MCPTT Group Size	The number of participants per MCPTT group call.																					
Use CRLF in flow csv	If enabled, it will use the CRLF line terminator in the generated CSV of the configured MCPTT flow. If disabled, it will use LF.																					
MCPTT Flow 	Press the <b>Open MCPTT Flow Editor</b> button to open the configuration page. Use the <b>Add New Row</b> button, and then select each column field to edit the flow.   <table border="1"> <thead> <tr> <th>Action Type</th> <th>Next Type</th> <th>Message URI</th> <th>Message Header</th> <th>Message Body</th> <th>Destination Host</th> <th>Destination Port</th> </tr> </thead> <tbody> <tr> <td>Send</td> <td>REGISTER</td> <td>REGISTER sip:n...</td> <td><input type="text"/></td> <td><input type="text"/></td> <td>12.0.0.2</td> <td>5080</td> </tr> <tr> <td>Send</td> <td>SUBSCRIBE</td> <td>SUBSCRIBE sip:n...</td> <td><input type="text"/></td> <td><input type="text"/></td> <td>12.0.0.2</td> <td>5080</td> </tr> </tbody> </table>	Action Type	Next Type	Message URI	Message Header	Message Body	Destination Host	Destination Port	Send	REGISTER	REGISTER sip:n...	<input type="text"/>	<input type="text"/>	12.0.0.2	5080	Send	SUBSCRIBE	SUBSCRIBE sip:n...	<input type="text"/>	<input type="text"/>	12.0.0.2	5080
Action Type	Next Type	Message URI	Message Header	Message Body	Destination Host	Destination Port																
Send	REGISTER	REGISTER sip:n...	<input type="text"/>	<input type="text"/>	12.0.0.2	5080																
Send	SUBSCRIBE	SUBSCRIBE sip:n...	<input type="text"/>	<input type="text"/>	12.0.0.2	5080																

## Advanced SIP Settings

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

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

### SIP Authentication

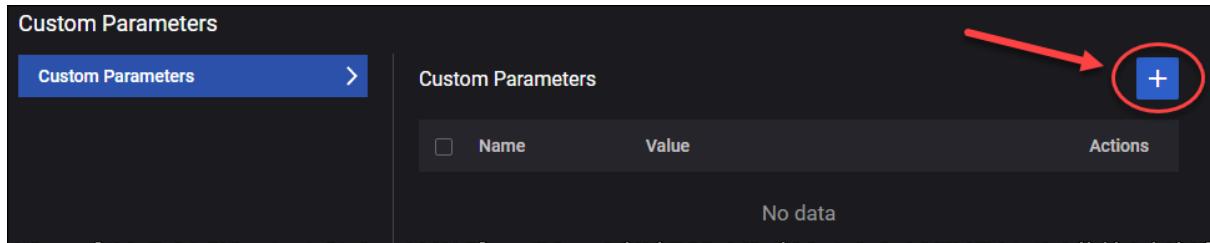
The parameters required for SIP authentication are presented in the table below.

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

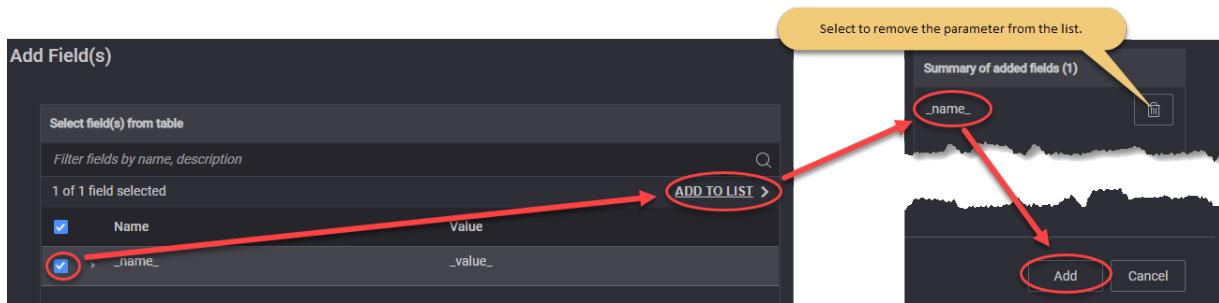
1. The Custom Parameters panel, select the **Add** button.



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"> <li>• <b>hmac-sha-1-96</b></li> <li>• <b>aes-gmac</b></li> <li>• <b>null</b></li> </ul>
Encryption Algorithm	Select the encryption algorithm: <ul style="list-style-type: none"> <li>• <b>aes-gcm</b></li> <li>• <b>aes-cbc</b></li> <li>• <b>null</b></li> </ul>

### 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 <b>Video OTT</b> .
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: <b>Simulated Users</b> or <b>Throughput</b> .
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: <b>IPv4</b> or <b>IPv6</b> .
Advanced OTT	Select the <b>Open Advanced OTT</b> button to enable and configure <a href="#">Advanced OTT Settings</a> .

## 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"> <li>To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul>
<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"> <li><b>DASH</b></li> <li><b>HLS</b></li> </ul>
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"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Quality Control</a> pane.
Advanced Client settings	These settings are presented in the <a href="#">Advanced Client Settings</a> 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: <b>Disabled</b> or <b>Mode 0</b> .
Quality Control Mode	Select the quality control mode from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Adaptive Bit Rate</b></li> <li>• <b>Quality Predefined Levels</b></li> <li>• <b>Lowest Quality</b></li> <li>• <b>Highest Quality</b></li> </ul>
Number of segments	This field is available and editable only when the Quality Control Mode is set to <b>Adaptive Bit Rate</b> .
<i>Play Profiles:</i> The following settings are available and editable only when the Quality Control Mode is set to <b>Quality Predefined Levels</b> .	

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"> <li>• <b>Stay at Current Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lowest Bitrate</b></li> <li>• <b>Change to the Lower Bitrate</b></li> <li>• <b>Change to the Higher Bitrate</b></li> </ul>
Numbers of levels to shift	This field is available and editable only when the Shift Type is set to <b>Change to Higher Bitrate</b> or <b>Change to Lower Bitrate</b> .
Play Until End	If this check box is selected, the <b>Play duration</b> field is disabled and the original playtime is used.
Play duration(sec)	This field is available only if the <b>Play Until End</b> check box is not selected. It allows you to set a custom playtime.

## Advanced Client Settings

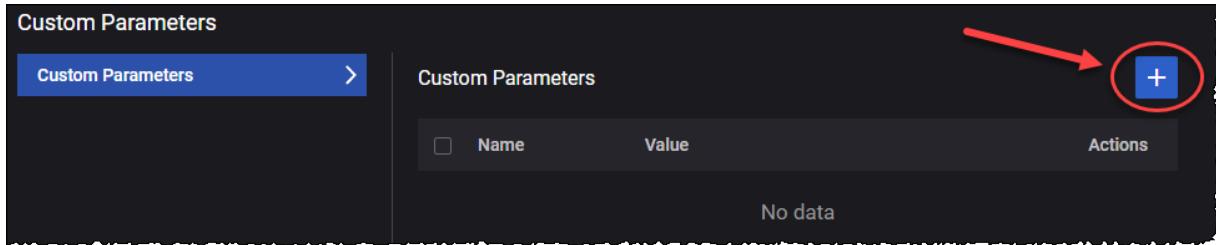
The parameters required for Advanced Client settings are presented in the table below.

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 <a href="#">Custom parameters</a> .

## Custom Parameters

You can add custom parameters as follows:

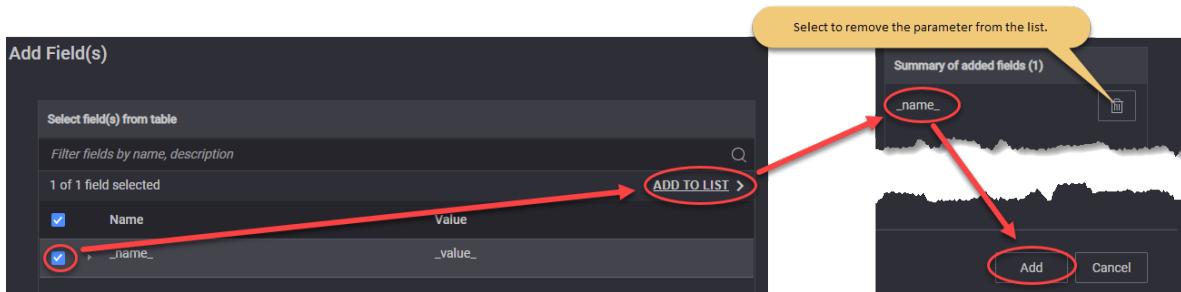
1. Select the **Open Custom Parameters** tile. The Custom Parameters panel opens.
2. Select the **Add** button.



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 <b>DNS Client</b> .
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 <b>Simulated Users</b> 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>

<b>Parameter</b>	<b>Description</b>
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: <b>IPv4</b> or <b>IPv6</b> .
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"> <li>• To select an existing traffic flow definition, click its name to open the Flow panel where you can view and modify the flow settings.</li> <li>• To add another traffic flow, click the <b>Add Flow</b> button. LoadCore will open the Flow panel where you will select the flow type and configure the flow settings.</li> </ul> <p>Refer to <a href="#">Flow</a> for a description of the configuration settings for these traffic flows. Also, you can add <a href="#">custom parameters</a>, based on your test configuration requirements.</p>

## Flow

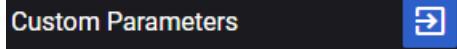
You can add and delete traffic flows as needed to meet your test objectives. The **Flow** parameters are described in the following table.

Parameter	Description
	Click the <b>Delete Flow</b> button to remove the flow from your configuration.
Type	By default, the type is set to <b>DNS Client</b> .
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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
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.
QoS FlowID	Select a QoS Flow ID for this flow.

## Custom Parameters

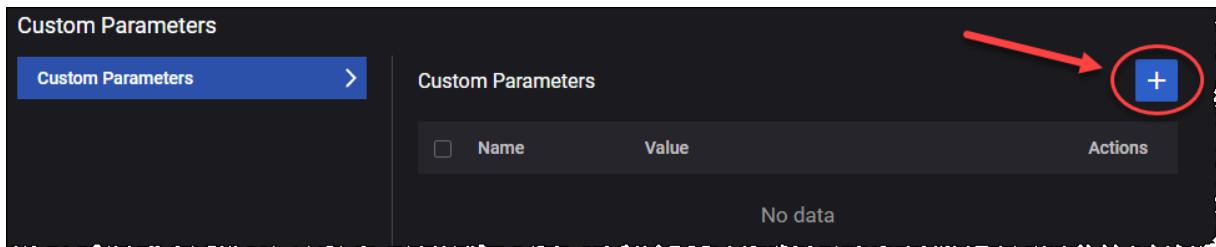
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

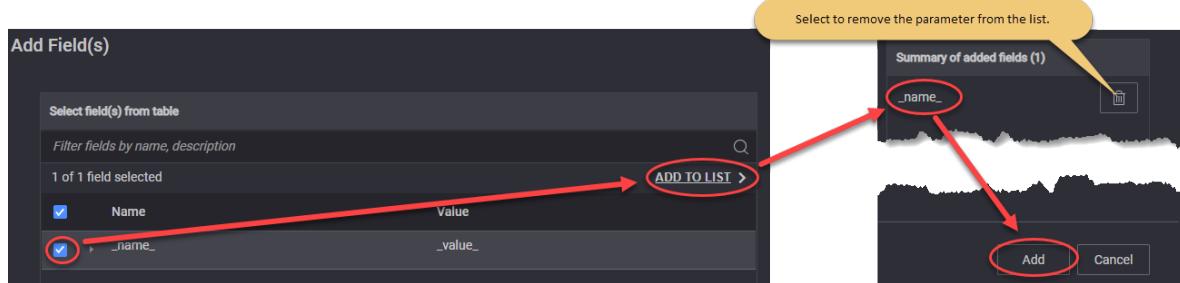
2. Select the **Add** button.



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 <b>ICMP Client</b> .
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 <b>Simulated Users</b> 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: <b>IPv4</b> or <b>IPv6</b> .
Traffic Flow	Refer to <a href="#">Traffic Flow</a> for a description of the configuration settings for these traffic flows.

## Traffic Flow

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

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

## Capture Replay

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

The following table describes the Capture Replay parameters.

Parameter	Description
Application Type	Select the application type. In this case, this parameter must be set to <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b>

Parameter	Description
	(option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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: <b>Initiator</b> and <b>Responder</b> .

Parameter	Description
	Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> (option disabled).
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to <b>Initiator</b> . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

## Synthetic

The following table describes the Synthetic parameters.

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

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

Parameter	Description
	number).

The following table describes the Traffic Flow parameters.

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: TCP or UDP.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Client Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
Server Burst Interval	The time interval at which the server sends packet bursts.
Server Burst Size (packets)	This field is available only when Transport Protocol is UDP. The number of packets the server sends in a burst.
Server Burst Size (bytes)	The packet size in bytes.
Server Timeout (ms)	This field is available only when Transport Protocol is UDP. Set the timeout value.
DNN	Select the DNN from the drop-down list.
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.

## UDG

The following table describes the UDG parameters.

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

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

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

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

Parameter	Description
<i>Flow</i>	
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>UDP</b> .
Out of Band Signaling	Select this check-box to enable OOB signaling. More details about the required parameters <a href="#">here</a> .  <b>IMPORTANT</b> To use the OOB feature, the OOB interface must be set in Agent Management window.
Destination Hostname	Destination hostname of the server. This value is editable.
Port	This represents the server(destination) port. This value is editable.
Client Source Port	The local port for client data connection.
Reconnect Timeout (ms)	The time interval after which the client attempts to reconnect after the connection was interrupted. 0 means that reconnect is disabled.
DNN	Select the DNN from the drop-down list.

Parameter	Description
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list.
<i>UDG Traffic Parameters</i>	<i>Select to enable and configure the <a href="#">UDG Traffic Parameters</a>.</i>
<i>Transaction</i>	<i>Select to enable and configure the <a href="#">Transaction</a> parameters.</i>
Status Query Interval	Timeout for keepalive packets on server. The server will wait for the <code>keepAliveInterval</code> value multiplied by <code>keepAliveExpiryCount</code> value.
Keepalive Interval	The time interval, in milliseconds, between UDG statistics requests (RESULT). A zero value means this feature is disabled.
Keepalive Expiry Count	The time to wait for UUDG to reconnect. A 0 value means the reconnect is disabled (in milliseconds).

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

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

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

Parameter	Description
UDG Test Type	Select the test type from the drop-down list. Available options: <b>Transmission</b> , <b>Ping-pong</b> or <b>Speed-Test</b> . For each test type, the parameters are described below.
<i>Transmission</i>	
Throughput Tx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change.

Parameter	Description
Client Burst Interval (ms)	The time interval at which the client sends packet bursts.
Client Burst Interval Unit	The unit in which this burst interval is expressed.
Client Burst Size (packets)	The number of packets the client sends in a burst.
Client Burst Size (bytes)	The packet size in bytes.
Throughput Rx (kbps)	This value is computed based on the parameters in the test and will be recalculated if one of these parameters change. A corresponding server is required to achieve the displayed value.
Server Burst Interval (ms)	The time interval at which the server sends packet bursts.
Server Burst Interval Unit	The unit in which this burst interval is expressed.
Server Burst Size (packets)	The number of packets the server sends in a burst.
Server Burst Interval Unit	Select the server burst interval unit. Available options: <b>Millisecond</b> or <b>Microsecond</b> .
Server Burst Size (bytes)	The packet size in bytes.
<i>Ping-pong</i>	
Ping Direction	Set the ping direction. Available options: <b>Upstream</b> or <b>Downstream</b> .
Ping Interval	Set the ping time interval.
Ping Interval Unit	Set the ping interval unit. Available options: <b>Millisecond</b> or <b>Microsecond</b> .
Pong Number	Set the value for the pong number.
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.
<i>Speed-Test</i>	
Traffic direction	Select the traffic direction for which this filter applies: <b>Uplink</b> or <b>Downlink</b> .

Parameter	Description
Client Packet Size (bytes)	The packet size in bytes.
Server Packet Size (bytes)	The packet size in bytes.

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

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

## REST API Client

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

The following table describes the REST API Client parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>REST API Client</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it with your own value.
Objective Type	This field is set to <b>Simulated Users</b> and cannot be modified.
Transport Protocol	Select the transport protocol from the drop-down list. Available options: <b>TCP</b> or <b>TLS</b> .
REST API Flow	The name of list of REST API Client sequential operations and transitions emulated by each REST API Client.  The REST API Flow is initially loaded into LoadCore's Resource Library, and then added to the test as a <a href="#">Global Playlists</a> . The list is defined in CSV format, following specific rules. Refer to <a href="#">Work with the Resource Library on page 73</a> section for further information.
Delay Application Traffic Start (ms)	The time (in milliseconds) to wait before starting the Attacks objective traffic.

Parameter	Description
IP Preference	Select a value from the drop-down list: <b>IPv4</b> or <b>IPv6</b> .
Iterations	If is set to <b>0</b> , it will be iterated on continuous loop during sustain time. If set to <b>1</b> , it will be executed only one time. <b>IMPORTANT</b> Values greater than 1 are not allowed.
Max Transactions per Connection	The maximum amount of transactions an application can make on one connection.
DNN	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
<i>TCP Settings</i>	
Min retransmission timeout (ms)	The lowest value that the computed RTO timer value can be set to. Expiry of the RTO timer indicates that the sender has not received an acknowledgment for the transmission, which triggers a retransmission of the segment. Upon each retransmission, the RTO timer value is doubled, up to the Max value. The default Min value is 2000 milliseconds and the permissible range of values is between 50 to 120000 milliseconds.
Max retransmission timeout (ms)	The highest value that the computed RTO timer value can be set to. The default value is 3200 milliseconds and the permissible range of values is between 1000 to 120000 milliseconds.
Receive buffer size (bytes)	The default size of the receive buffer (in bytes). This parameter affects the TCP receive window size. If you increase the size of the receive buffer, then the receive window is prolonged. If you are experiencing high latency on your test network, increase the size of the receive buffer to improve the throughput.
Transmit buffer size (bytes)	The default size of the transmit buffer (in bytes). This parameter affects the TCP transmit window size. If you increase the size of the transmit buffer, the transmit window is prolonged. If you are experiencing high latency on your test network, increase the size of the transmit buffer to improve the throughput.
Min Source Port	The source port specifies which ports are used for client connections. The Min value specifies the lower bound (the lowest permissible port number).
Max Source Port	The Max value specifies the upper bound (the highest permissible port number).
MSS	The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated, specified in bytes.

Parameter	Description
	The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size minus the IP header size. For example, for traditional Ethernet, the MSS value is 1460 (1500 minus 40).
Selective Acknowledgments	Select the toggle button to enable this option.
TLS Settings	See <a href="#">TLS Settings</a> table for more details.
Custom Parameters	For more details, refer to <a href="#">Custom parameters</a> .

## TLS Settings

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

Parameter	Description
	<b>IMPORTANT</b> This parameter becomes available only if TLSv1.3 is selected.
Immediate close	Select the check box to enable it.
Send close notify	If enabled, it will send a close notify message.

## Custom Parameters

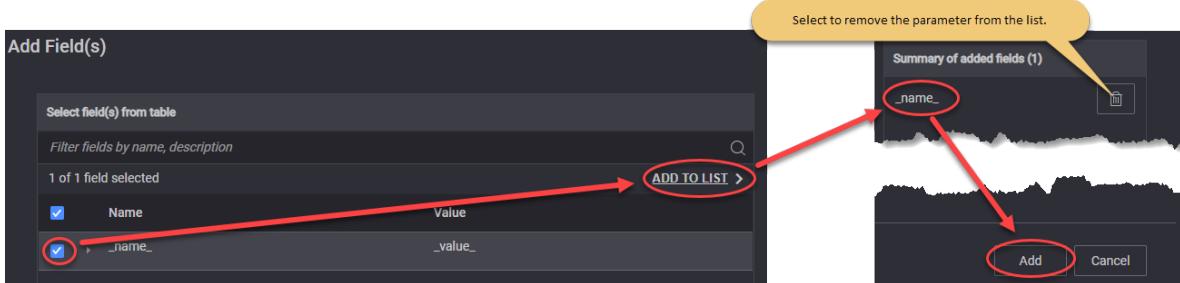
From this section you can add custom parameters fields:

- **Custom Parameters**

You can add custom parameters as follows:

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

**For example ...**



## How to Configure the REST API Client

1. Define your REST API flow in an CSV file, following the rules described in the [REST Client Flow specifications](#).
2. Load the CSV as a Global Playlist in LoadCore user interface:
  - a. Go to **Global Settings > Global Playlist**.
  - b. Add a new Playlist using the **+** button.
  - c. **Name** the new Playlist - it will be used in the REST API Client application configuration.
  - d. **Upload** the CSV created at **Step 1**.
3. In the User Plane UE section, select the **REST API Client** application traffic.
4. Set all necessary parameters on required by the application (see [REST API parameters table](#) above):

- on **Transport protocol** select **TCP** or **TLS** (version 1.2 and 1.3 configurable from TLS Settings).
- the **Objective type** is automatically set to **Simulated users**.
- add the **REST API Flow** name that defines the REST sequence of actions defined in the Global Playlist.
- set the **Max Transactions per Connection**- for REST API Client application, one "Transaction" points to all REST actions (HTTP requests) specified in REST flow.
- Set all other common parameters.

## REST Client Flow specifications

The REST Client flow will be specified in CSV format state-by-state. For each State in flow, three main commands must be specified, and one special command at the end of list:

Command	Condition	Description
<b>Action</b>	Mandatory	<p>Indicates what actions should be executed in the current State and what transitions can be executed. The following rules are in place:</p> <ul style="list-style-type: none"> <li>• up to 4 transitions are allowed. Maximum 4 pairs of (Conditions, NextState) are used from CSV.</li> <li>• Method, Headers and Body should be specified in separate columns.</li> <li>• Method, Headers and Body can contain dynamic parts specified by flow user variables.</li> </ul>
<b>Extract</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>Specifies if some elements from the last HTTP response should be extracted in user variables for further utilization in flow:</p> <ul style="list-style-type: none"> <li>• extractions are specified using (backqoute_separated_path, userVar) pairs.</li> <li>• up to 3 extractions per REST(HTTP) response are allowed.</li> </ul>
<b>Statistics</b>	Optional	<p><b>NOTE</b> This row must exist, but can be empty.</p> <p>User-defined Counters can be incremented when the condition is fulfilled. The configuration is done in pairs of (condition, UserCounter).</p>
<b>ENDMARKER</b>	Mandatory	This special command is mandatory to indicate the end of REST API flow. No other command will be executed after the ENDMARKER was executed. It can be inserted anywhere in the Playlist, on the first column.

## REST user flow variables

There are 10 flow variables with predefined names (`userVar1`, `userVar2`, ..., `userVar10`) available for store extracted values from REST Commands during flow duration. On each REST Command, you can configure what to extract from the received Response, and in what variable.

Each variable can be overwritten at anytime, therefore a variable can be persistent during the flow duration, or only temporary, until overwrite.

## Predefined Applications Traffic

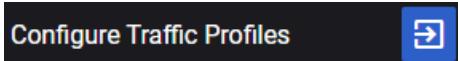
The following table describes the Predefined Flows Traffic parameters.

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Predefined Applications</b> .
Objective Type	Select an option from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Simulated Users</b></li> <li>• <b>Throughput</b></li> <li>• <b>Connections Per Second</b></li> </ul>
Throughput (kbps)	<p><b>IMPORTANT</b> This parameter is available only when <a href="#">Objective Type</a> is set to <b>Throughput</b>.</p> <p>The desired throughput (in kbps) for the combined traffic flows that will be generated.</p>
Connections Per Seconds	<p><b>IMPORTANT</b> This parameter is available only when <a href="#">Objective Type</a> is set to <b>Connections Per Second</b>.</p> <p>Set the number of connections.</p>
MSS	<p>The desired Maximum Segment Size (MSS) for the user plane traffic that will be generated for this UE range, specified in bytes.</p> <p>The MSS is the largest TCP segment that the IP device can transmit as a single, unfragmented unit. It is typically calculated as the MTU minus the TCP header size 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.
Configure Traffic Profiles	<p>Each Application Traffic entry requires at least one traffic profile definition, and can support multiple such definitions.</p> <p>Refer to <a href="#">Traffic Profile</a> for a description of the configuration settings for these traffic profiles.</p>

## Traffic Profile

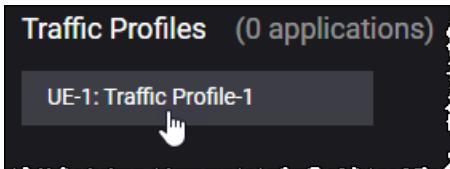
You can configure the traffic profiles as needed to meet your test objectives. You can do this as follows:

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



The Traffic Profiles section opens.

2. Select the Traffic Profiles tile.



The Traffic Profile Configuration section opens.

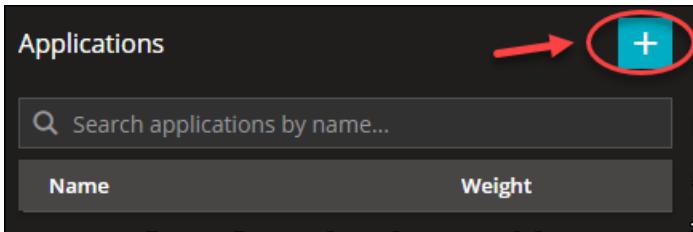
3. From the Predefined Applications sections, you can add and configure applications by selecting the following sections:

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

## Applications

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

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



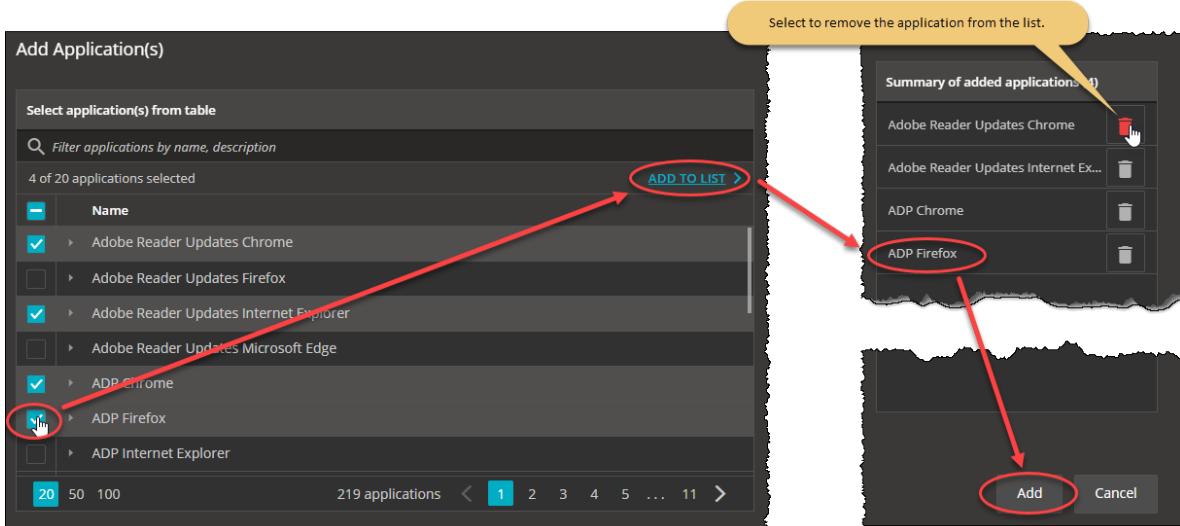
The Add Application(s) window opens.

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

**NOTE**

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

**For example ...**



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

**For example ...**

Name	Weight	Action Buttons
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 <b>Throughput</b> , 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"> <li>• <b>Rename</b> - Select to rename the application.</li> <li>• <b>Advanced Settings</b> - for more information, refer to <a href="#">Advanced Settings</a>.</li> <li>• <b>Delete</b> - Select to delete the application.</li> </ul>

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

### For example ...

The screenshot shows the 'Applications' management interface. On the left, there is a search bar and a table listing applications with columns for Name and Weight. One row is selected, showing 'Adobe Reader Updates Chrome 1'. On the right, the 'Application Settings' section displays fields for Destination Hostname, DNN ID, and QoS Flow ID. Below it, the 'Application Actions' section shows a list of actions with their names and descriptions:

#	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.

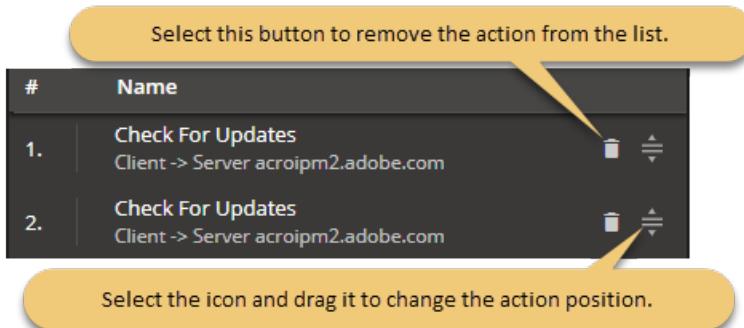
### Application Actions

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.

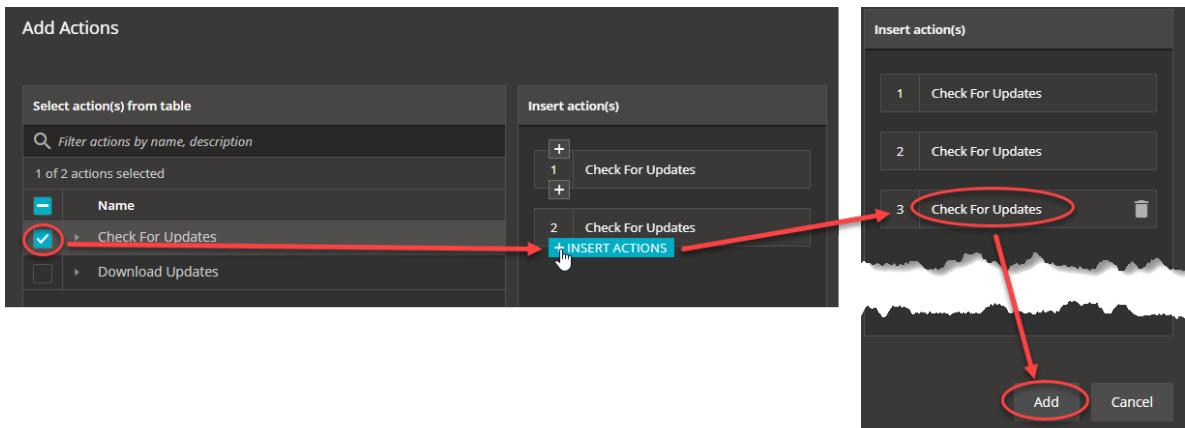
### For example ...



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 ...**



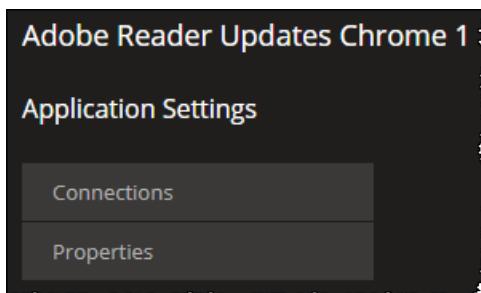
3. If needed, you can select the **Edit** button to enable the bulk selection of the available actions in order to remove them from the list.

## 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.

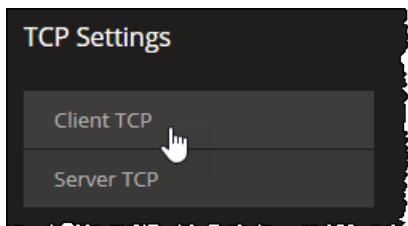
Under the **Properties** section, the application settings Properties fields are displayed, as follows:

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"> <li>• Chrome</li> <li>• Firefox</li> <li>• Opera</li> <li>• Microsoft Edge</li> <li>• Internet Explorer</li> <li>• Safari</li> <li>• Android</li> </ul>
Action Timeout (seconds)	Set the action timeout in seconds.
Connection Persistence	Select an option for the connection persistence: <ul style="list-style-type: none"> <li>• <b>Standard</b> - inherits the behavior with respect to the HTTP version (1.0 or 1.1).</li> <li>• <b>Disabled</b> - enforces connection closing following every HTTP message.</li> <li>• <b>Enabled</b> - enforces connection persistence through explicit keep-alive.</li> </ul>

Field	Description
HTTP Version	Select the HTTP version used: <ul style="list-style-type: none"> <li>• <b>HTTP/1.0</b></li> <li>• <b>HTTP/1.1</b></li> </ul>

## TCP Settings

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



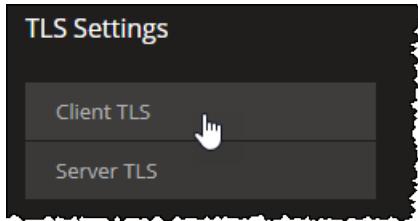
These parameters are configurable for both Client and Server settings, as presented in the following table.

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 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.

Parameter	Description
Enable RFC1323 TCP timestamps	<p>Enable or disable the stamp using the toggle button. If enabled, the client or server inserts an RFC 1323 timestamp into each packet.</p> <p><b>NOTE</b> 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
<i>TLSv1.2</i>	<p>Select the check box to enable it. The following options became available:</p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Disable</li> <li>• Session ticket</li> <li>• Session ID</li> </ul> <p><b>NOTE</b> Session reuse method is available only if <i>TLSv1.2</i> is selected.</p>

Parameter	Description
Immediate close	Select the check box to enable it.
TLSv1.3	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	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	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Session reuse method	<p>Select the Session Reuse Method from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Disable</li> <li>• Session ticket</li> <li>• Session ID</li> </ul> <p><b>NOTE</b> Session reuse method is available only if TLSv1.2 is selected.</p>
Immediate close	Select the check box to enable it.
TLSv1.3	<p><i>Select the check box to enable it.</i></p> <p><i>The following options became available:</i></p>
Cipher	Select one or more ciphers from the drop-down list.
Middlebox compatibility	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.
SNI Enabled	<i>Select the check box to enable the server name indicator. The following <b>SNI Settings</b> become available:</i>
Certificate file	Select <b>Upload</b> to add your certificate file or <b>Clear</b> to remove it.

Parameter	Description
Key file	Select <b>Upload</b> to add your key file or <b>Clear</b> to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select <b>Upload</b> to add your DH file or <b>Clear</b> to remove it.
Certificate file	Select <b>Upload</b> to add your certificate file or <b>Clear</b> to remove it.
Key file	Select <b>Upload</b> to add your key file or <b>Clear</b> to remove it.
Key file password	Enter your key file password.
DH file Traffic	Select <b>Upload</b> to add your DH file or <b>Clear</b> 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: <b>None</b> , <b>XOR</b> , <b>ZOOM</b> or <b>SRTP</b> .
MOS Mode	Select the Session Reuse Method from the drop-down list. Available options: <b>Disable</b> , <b>Per interval</b> or <b>Per call</b> .

## 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:

<b>DN Ranges panel</b> .....	<b>1131</b>
<b>DN Range panel</b> .....	<b>1131</b>
<b>DN N6 interface settings</b> .....	<b>1132</b>
<b>DN routes settings</b> .....	<b>1133</b>
<b>DN User Plane</b> .....	<b>1134</b>
DN Stateless UDP Traffic .....	1135
DN Data Traffic .....	1137

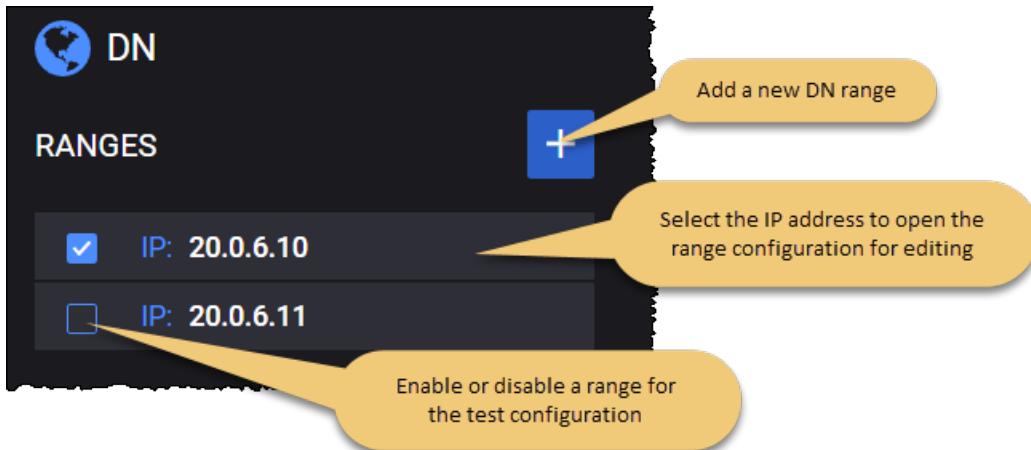
DN Voice Traffic .....	1139
DN Video OTT Traffic .....	1150
DN DNS Server Traffic .....	1153
DN Predefined Applications Traffic .....	1156
DN Capture Replay .....	1156
DN Synthetic .....	1158
<b>DN Throttling settings .....</b>	<b>1160</b>

## 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 ...



If multiple agents are assigned to the DN node, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

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

## 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 <b>Delete Range</b> 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 <a href="#">DN N6 interface settings</a> .
Routes Settings	These settings are described in <a href="#">DN routes settings</a> .
User Plane	These settings are described in <a href="#">DN User Plane</a> .
Throttling Settings	These settings are described in <a href="#">DN Throttling settings</a> .

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

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

## DN routes settings

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

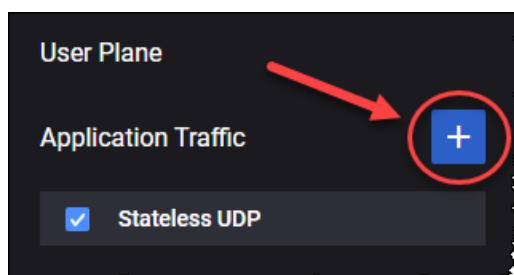
The following table describes the **Route Settings** that you need to configure in order to create the route to an UE or custom range.

Settings	Description
<i>Routes Config:</i>	

Settings	Description
	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: <b>UE</b> or <b>Custom</b> .
UE Range MSIN	Select the MSIN of the UE range from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .
Peer UPF/SGW	Select the UPF node connected to DN over the N6 interface from the drop-down list. This parameter is available only when the route type is set to <b>UE</b> .
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"> <li>• All: Select this item to choose all of the available DNNs that are configured for the UE.</li> <li>• specific DNNs: Select one or more of the individual DNNs from the list.</li> </ul> This parameter is available only when the route type is set to <b>UE</b> .
Destination Subnet Address	Set the destination subnet address. This parameter is available only when the route type is set to <b>Custom</b> .
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 <b>Custom</b> .

## 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](#).

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

## DN Stateless UDP Traffic

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

Parameter	Description
Application Type	Select the type of traffic you want to generate. In this case, this parameter must be set to <b>Stateless UDP</b> .
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 <b>downlink</b> 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 <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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 <b>Data</b> .
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"> <li>• To select an existing application server definition, click its name to open the Server panel where you can view and modify the server settings.</li> <li>• To add another application server, click the <b>Add Server</b> button. LoadCore will open the Server panel where you will select the server type and configure the server settings.</li> </ul> <p>Refer to <a href="#">Server</a> (below) for a description of the configuration settings required by the application server.</p> <p>Also, you can add <a href="#">custom parameters</a>, 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 <b>Delete Server</b> 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: <b>TCP</b> , <b>TLS</b> , <b>QUIC</b> or <b>UDP</b> .
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"> <li>For <b>TCP</b> transport protocol: <b>HTTP Get Responder</b>, <b>HTTP Put Responder</b>, <b>HTTP Post Responder</b>, <b>HTTP Server</b> and <b>FTP Responder</b>.</li> <li>For <b>TLS</b> transport protocol: <b>HTTPS Get Responder</b>, <b>HTTPS Put Responder</b>, <b>HTTPS Post Responder</b> and <b>HTTPS Server</b>.</li> <li>For <b>QUIC</b> transport protocol: <b>HTTP3 Server</b>.</li> <li>For <b>UDP</b> transport protocol: <b>UDP Bidirectional Responder</b>.</li> </ul>
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

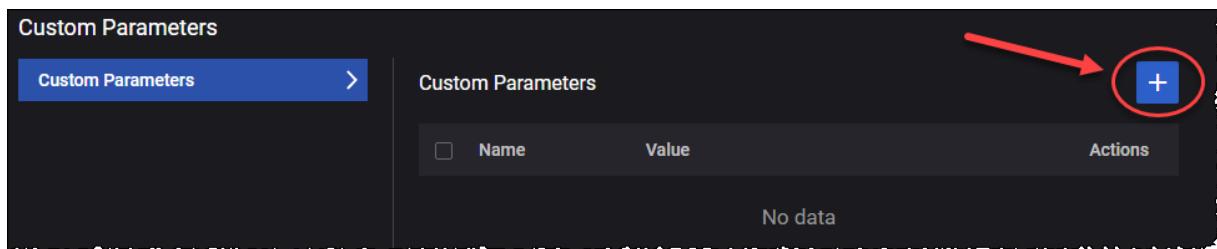
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

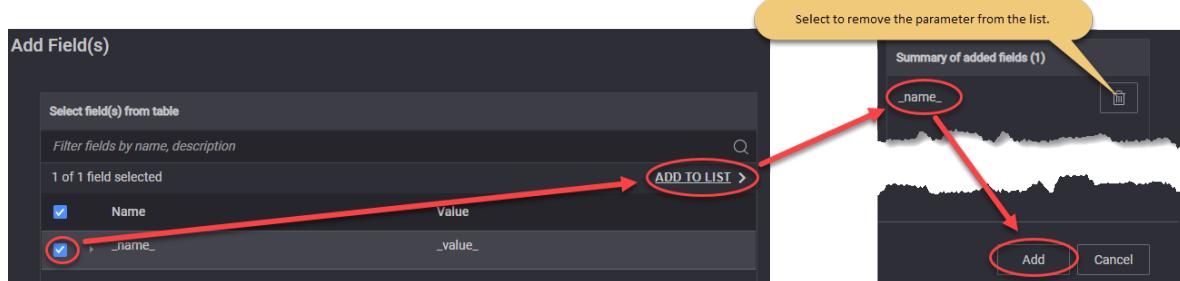
2. Select the **Add** button.



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 <b>Voice</b> .
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 <b>Simulated Users</b> and cannot be changed.
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 <a href="#">Dial Plan</a>.</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"> <li><b>TCP</b> - Transmission Control Protocol</li> <li><b>TLS</b> - Transport Layer Security</li> <li><b>UDP</b> - User Datagram Protocol</li> </ul>

Parameter	Description
Domain	Provide the domain name.
Advanced SIP Settings	For more details about these settings, refer to <a href="#">Advanced SIP Settings</a> .
<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.
Enable SRTP	Select this option in order to enable Secure Real-time Transport Protocol (SRTP).
RTP Session Duration (ms)	Set the value for the session duration.
Audio settings:	<i>For the configuration of audio settings, refer to <a href="#">Audio Settings</a>.</i>
Video Settings:	<i>For the configuration of video settings, refer to <a href="#">Video Settings</a>.</i>
MSRP Settings:	<i>For the configuration of MSRP settings, refer to <a href="#">MSRP Settings</a>.</i>
MCTTP Settings	<i>For the configuration of MCTTP settings, refer to <a href="#">MCPTT Settings</a>.</i>
<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"> <li>• <b>None</b></li> <li>• <b>EVS/AMR IPv4</b></li> <li>• <b>NB Codecs IPv6</b></li> <li>• <b>AMR-WB IPv6</b></li> <li>• <b>Multimedia IPv4</b></li> </ul>
QoE Settings	<i>Select this panel to open the audio QoE settings.</i>
Enable MOS	Select this option to enable MOS (Mean Opinion Score).

## Dial Plan

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

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

## Audio Settings

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

Parameter	Description
Enable Audio	Select to enable this option.
QoS Flow ID for Voice	Select the QoS flow used 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"> <li>• <b>AMR</b> - 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.</li> <li>• <b>AMR-WB</b> - 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.</li> <li>• <b>EVS</b> - 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.</li> <li>• <b>PCMU</b></li> <li>• <b>PCMA</b></li> <li>• <b>iLBC</b></li> </ul>

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

### AMR/AMR-WB

Parameter	Description
Packet Time (ms)	Length of time in milliseconds represented by the media in a packet. AMR speech encoding is performed on 20 ms speech frames.
Payload Type	Specifies the audio payload type.
Payload Format	<p>For a given session, the payload format can be either bandwidth efficient or octet aligned, depending on the mode of operation that is established for the session via out-of-band means.</p> <ul style="list-style-type: none"> <li>• <b>Bandwidth efficient:</b> In the bandwidth efficient format only the full payload is octet aligned, so fewer padding bits are added.</li> <li>• <b>Octet aligned:</b> 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.</li> </ul>
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"> <li>• <b>Full header</b> - 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.</li> <li>• <b>Compact</b> - In this payload format a single codec data frame is sent in each RTP packet. The format uses protected payload sizes that uniquely identify</li> </ul>

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

### PCMU/PCMA/iLBC/G722/G723/G729

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

### Video Settings

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

Parameter	Description
Enable video	Select to enable this option.
QoS Flow ID for Video	Select the QoS Flows ID(s) from the drop-down list.
Video Codecs	<i>This section is available only when <b>Enable video</b> 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: <b>H264</b> or <b>H265</b> .
FPS	Set the FPS value.
Payload Type	Set the payload type value.
Average Bitrate (kbps)	Set the average bit rate value.

### MSRP Settings

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

Parameter	Description
Enable MSRP	Select to enable this option.

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

## MCPTT Settings

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

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

## Advanced SIP Settings

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

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

### SIP Custom Headers

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

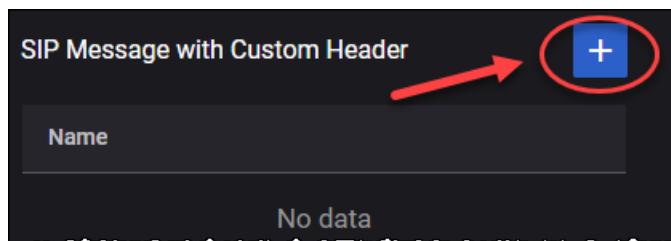
**NOTE**

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

For each message, you can:

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

- Select the **Add** button.



The Add Field(s) opens.

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

**For example ...**

The following custom header are available:

Parameter	Description	Value
Accept	IETF RFC 3261	application/sdp,message/cpim
Accept-Contact	IETF RFC 3841	*;mobility="mobile";methods="INVITE"
Accept-Encoding	IETF RFC 3261	gzip
Accept-Language	IETF RFC 3261	da, en-gb;q=0.8, en;q=0.7
Alert-Info	IETF RFC 3261	:<urn:alert:service:call-waiting>
Allow	IETF RFC 3261	INVITE, ACK, UPDATE, PRACK, CANCEL, PUBLISH, MESSAGE, OPTIONS, SUBSCRIBE, NOTIFY

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
Allow-Events	IETF RFC 6665	conference
Authentication-Info	IETF RFC 3261, IETF RFC 3310	nexnonce="47364c23432d2e131a5fb210812c"
Call-Info	IETF RFC 3261	<http://www.example.com/alice/photo.jpg> ;purpose=icon
Content-Disposition	IETF RFC 3261	session
Content-Encoding	IETF RFC 3261	gzip
Content-ID	IETF RFC 8262	<target123@atlanta.example.com>
Content-Language	IETF RFC 3261	fr
Date	Sat,13 Nov 2010 23:29:0 0 GMT	IETF RFC 3261
Error-Info	IETF RFC 3261	<sip:announcement10@example.com>
Event	IETF RFC 6665, IETF RFC 6446, IETF RFC 3680	reg
Expires	IETF RFC 3261	3600
Feature-Caps	IETF RFC 6809, 3GPP TS 24.229	+3gpp.trf=sip:trf3.operator3.com
Geolocation	IETF RFC	<user1@operator1.com>

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
n	IETF RFC 3261	6442
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-Associate-d-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

<b>Parameter</b>	<b>Description</b>	<b>Value</b>
P-Preferred-Identity	IETF RFC 3325	"Cullen Jennings" <sip:fluffy@cisco.com>
P-Preferred-Service	IETF RFC 6050	urn:urn-7:3gpp-service.ims.icsi.mmTEL
Priority	IETF RFC 3261	emergency
Proxy-Authenticate	IETF RFC 3261	Digest realm="atlanta.com",domain="sip:ss1.carrier.com",qop="auth",nonce="f84f1cec41e6cbe5aea9c8e88d359",opaque="",stale=False,algorithm=MD5
Proxy-Authorization	IETF RFC 3261	Digest username="Alice",realm="atlanta.com",nonce="c60f3082ee1212b402a21831ae",response="245f23415f11432b3434341c022"
Proxy-Require	IETF RFC 3261	foo
P-Visited-Network-ID	IETF RFC 7315	Visited network number 1
RAck	IETF RFC 3262	10
Reason	IETF RFC 3326	Q.850;cause=16;text="Terminated"
Record-Route	IETF RFC 3261	<sip:server10.biloxi.com;lr>, <sip:bigbox3.site3.atlanta.com;lr>
Refer-To	IETF RFC 3515	<sip:dave@bobster.example.org?Replaces=425928%40bobster.example.com.3%3Btag%3D7743%3Bfrom-tag%3D6472>
Reply-To	IETF RFC 3261	Bob <sip:bob@biloxi.com>
Request-Disposition	IETF RFC 3841	proxy
Require	IETF RFC 3261	Path

Parameter	Description	Value
Retry-After	IETF RFC 3261	3600
Route	IETF RFC 3261	<sip:bigbox3.site3.atlanta.com;lr>,<sip:server10.biloxi.com;lr>
RSeq	IETF RFC 3262	10
Server	IETF RFC 3261	HomeServer v2
Service-Route	IETF RFC 3608	<sip:P2.HOME.EXAMPLE.COM;lr>
Session-Expires	IETF RFC 4028	3600;refresher=uac
Session-ID	IETF RFC 7329	0123456789abcdef123456789abcdef0
SIP-Etag	IETF RFC 3903	12345
SIP-If-Match	IETF RFC 3903	12345
Subject	IETF RFC 3261	Need more boxes
Subscription-State	IETF RFC 6665	active
Supported	IETF RFC 3261	100Rel,timer,precondition
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"> <li>• <b>Digest MD5</b></li> <li>• <b>AKAv1</b></li> <li>• <b>AKAv2</b></li> <li>• <b>ProxyDefined</b></li> </ul>
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 <b>Video OTT</b> .
Label	Set the label name. You can accept the value provided by LoadCore or overwrite it

Parameter	Description
	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).
<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"> <li>• <b>HTTP</b></li> <li>• <b>HTTPS</b></li> <li>• <b>HTTP/QUIC</b></li> </ul>
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 <a href="#">Streams</a> (below) for descriptions of the OTT server streams settings.
Custom Parameters	You can add <a href="#">custom parameters</a> , 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.

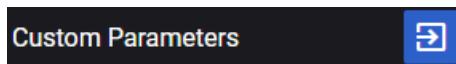
Parameter	Description
	Select this button to add a stream to your test configuration.

Parameter	Description
	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"> <li>• <b>Real</b></li> <li>• <b>Synthetic</b></li> </ul>
Protocol	Select the protocol from the drop-down list: <ul style="list-style-type: none"> <li>• <b>Apple HLS</b></li> <li>• <b>DASH</b>.</li> </ul> If the stream type is set to <b>Synthetic</b> , you can choose one protocol from list. If the stream type is set to <b>Real</b> , you will see the protocol of real stream loaded.
Stream Duration	If the stream type is set to <b>Synthetic</b> , you can configure the stream duration in seconds. If the stream type is set to <b>Real</b> , you will see the real stream duration.
Segment Duration	If the stream type is set to <b>Synthetic</b> , you can configure the segment duration in seconds. If the stream type is set to <b>Real</b> , 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: <b>QCIF, 240p, nHD, 480, WXGA, FHD, QHD, 4K, 8K</b> .
Frames per second	Set the number of frames per second.

## Custom Parameters

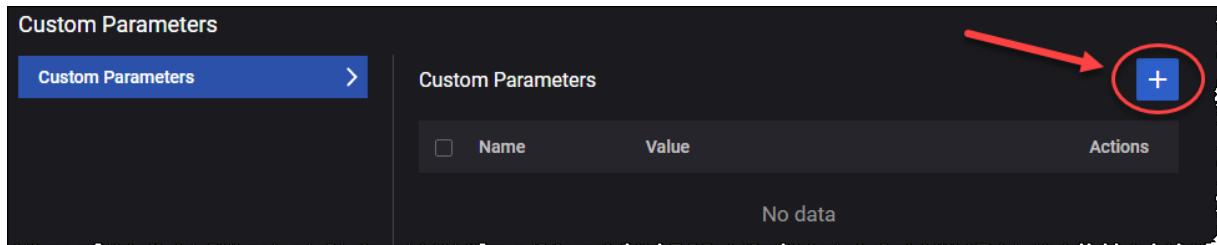
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

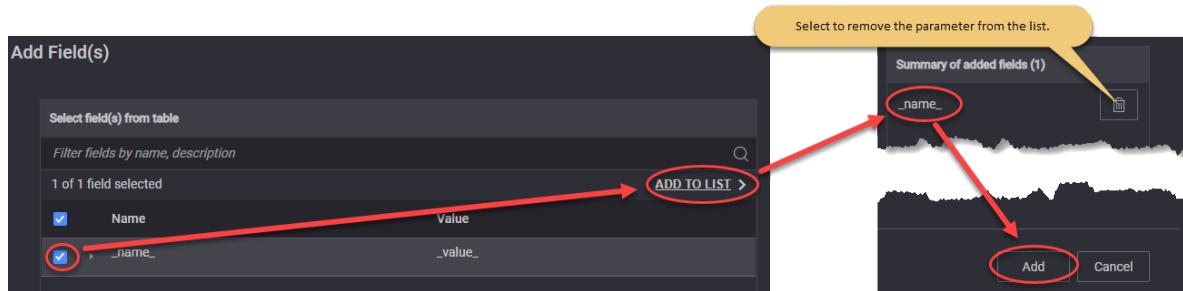
2. Select the **Add** button.



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 <b>DNS Server</b> .
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).

Parameter	Description
<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 <a href="#">Zone Manager</a> for descriptions of the DNS server zones settings.</i>
Custom Parameters	<i>You can add <a href="#">custom parameters</a>, 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.

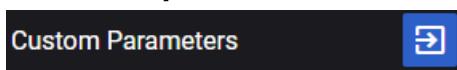
Parameter	Description
	Select this button to add a zone to your test configuration.
	Select this button to remove the zone from the test configuration.
Zone Name	Set the zone name. Each zone is identified by a unique name. You can accept the value provided by LoadCore or overwrite it with your own value.
Master Server	Provide the value for the master server.
Resource Records (RRs)	
	Select this button to add a resource record to your test configuration.

Parameter	Description
	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"> <li>• <b>A</b></li> <li>• <b>AAAA</b></li> <li>• <b>CNAME</b></li> <li>• <b>TXT</b></li> <li>• <b>PTR</b></li> <li>• <b>NS</b></li> </ul>
Hostname	Set the hostname.
Address	Provide the address.

## Custom Parameters

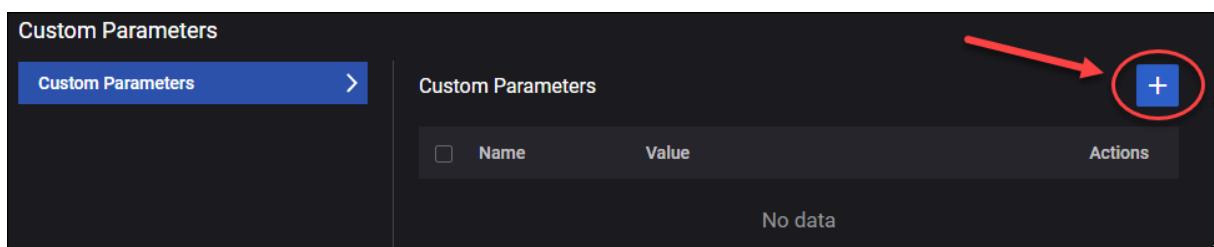
You can add custom parameters as follows:

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



The Custom Parameters panel opens.

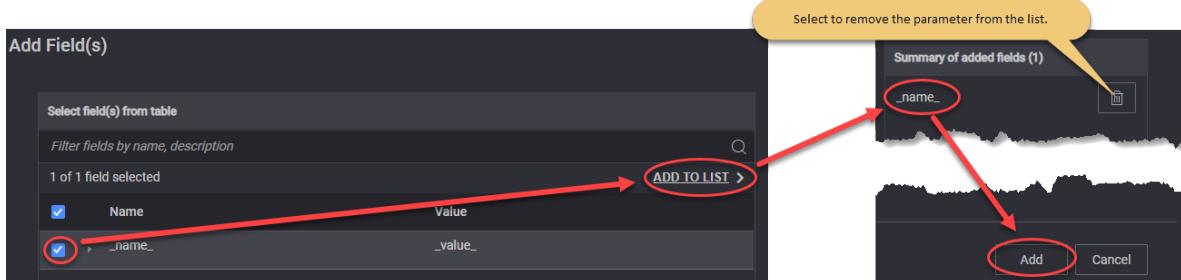
2. Select the **Add** button.



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 <b>Predefined Applications</b> .
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 <b>Capture Replay</b> .
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 <b>Upload</b> button. To remove the file, select the <b>Clear</b> button.
Iterations	The number of times the capture will be replayed for each subscriber. Set to <b>0</b> for no limit. The default value is <b>1</b> .
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 <b>1000</b> 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 <b>true</b>

Parameter	Description
	(option enabled).
Resynchronize	Try to resync responder with initiator by matching incoming packets ahead and behind the current packet. The default value is <b>true</b> (option enabled).
Start Delay (s)	The number of seconds to wait from the start of sustain time (i.e. after all UEs have registered).
DNN ID	Select the DNN value for the drop-down list. For more details about DNN configuration, refer to <a href="#">DNN configuration settings</a> .
QoS Flow ID	Select the QoS Flows ID(s) from the drop-down list. For more details about QoS Flow configuration, refer to <a href="#">QoS Flow configuration settings</a> .
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"> <li>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.</li> <li>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).</li> </ul> <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: <b>Initiator</b> and <b>Responder</b> .

Parameter	Description
	Default value: <b>Initiator</b> .
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 <a href="https://www.tcpdump.org/manpages/pcap-filter.7.html">https://www.tcpdump.org/manpages/pcap-filter.7.html</a> .
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 <b>false</b> (option disabled).
<i>Overrides</i>	
Override QoS Flow ID	This option is available only if the <i>Role</i> is set to <b>Initiator</b> . Select the toggle button to enable it.
Qos Flow ID	This option is available only when <i>Override QoS Flow ID</i> option is enabled. Select the QoS Flows ID(s) from the drop-down list.
Override IP Address	Select the toggle button to enable it. When enabled, <i>Destination IP Address</i> and <i>Destination IP Address Count</i> fields become available.
Destination IP Address	The destination IP address to place in the IP packet.
Destination IP Address Count	The destination IP address count value.

## DN Synthetic

The following table describes the Synthetic parameters.

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

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

The following table describes the Traffic Flow parameters.

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

## DN Throttling settings

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

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

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

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

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

## 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:**

<b>CSCF Range panel</b> .....	<b>1161</b>
<b>Media Function Range panel</b> .....	<b>1162</b>

## CSCF Range panel

When you select the 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.
Force IPsec Null Encryption	If enabled, it forces IPsec null encryption, therefore not encrypting the ESP traffic.
<i>Authentication Settings</i>	
Enable Authentication	Select this option to enable authentication.
Realm	Set the realm. Default value: <b>keysight.com</b> .
Algorithm Type	Select the algorithm type from the drop-down list. Available options: <b>Digest</b> , <b>AKAv2</b> or <b>AKAv1</b> .
Algorithm	Select the algorithm from the drop-down list. Available options: <b>MD5</b> , <b>MD5-Sess</b> , <b>SHA256</b> or <b>SHA256-Sess</b> .
Quality of Protection	Select an option from the drop-down list: <b>auth</b> or <b>auth-init</b> .
<i>Connectivity Settings</i>	

Setting	Description
IP Address	Set the IP address.

## Media Function Range panel

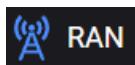
When you select the Media Function's IP address from the **Media Function Ranges** panel, LoadCore opens the **Range** panel, from which you can configure the connectivity settings for the Media Function range.

### Media Function range controls and settings

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

Connectivity Settings	Description
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.

## RAN/Untrusted AP configuration settings



In wireless networks, a Radio Access Network (RAN) is the network that enables user endpoints, such as mobile phones, to communicate and access core network resources. The 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. In 5G topology, an *untrusted AP* refers to an Access Point that is considered unsecure or not fully trusted by the cellular network operator.

The configuration settings are described in the topics listed below.

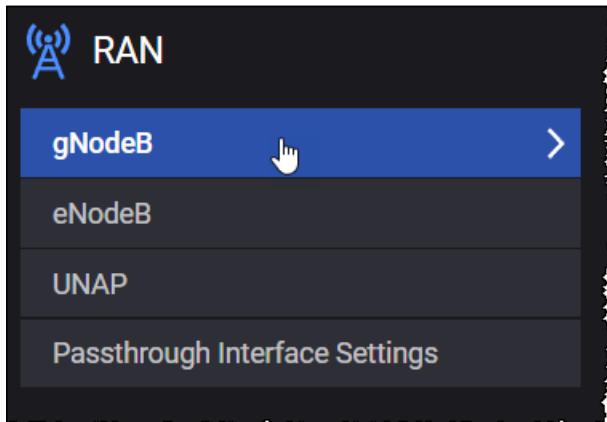
### Topics:

<b>gNodeB</b> .....	<b>1163</b>
gNodeB Ranges panel .....	1163
gNodeB Range settings .....	1167
gNodeB node settings .....	1168
gNodeB NSSAI settings .....	1170
gNodeB N2 interface settings .....	1172
gNodeB N3 interface settings .....	1176
<b>eNodeB</b> .....	<b>1180</b>
eNodeB Ranges panel .....	1180
eNodeB Range Settings .....	1184
eNodeB Node Settings .....	1185
S1-U Interface Settings .....	1186

S1-MME Interface Settings .....	1187
<b>UNAP .....</b>	<b>1190</b>
UNAP Ranges panel .....	1190
UNAP Range Settings .....	1191
<b>Passthrough interface settings .....</b>	<b>1193</b>

## 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:

<b>gNodeB Ranges panel .....</b>	<b>1163</b>
<b>gNodeB Range settings .....</b>	<b>1167</b>
<b>gNodeB node settings .....</b>	<b>1168</b>
<b>gNodeB NSSAI settings .....</b>	<b>1170</b>
<b>gNodeB N2 interface settings .....</b>	<b>1172</b>
<b>gNodeB N3 interface settings .....</b>	<b>1176</b>

## gNodeB Ranges panel

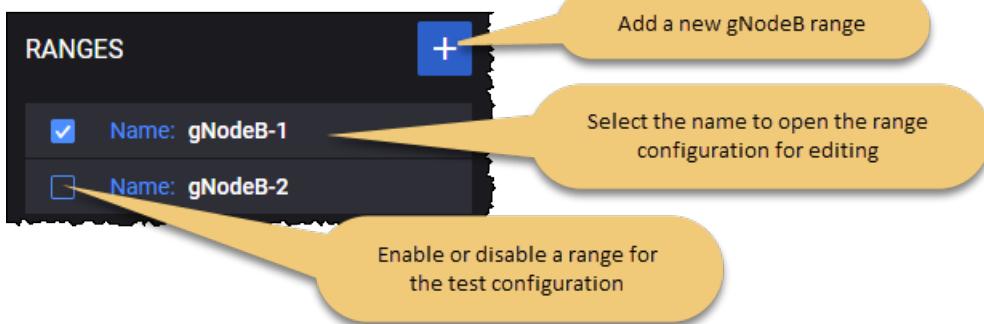
The **gNodeB Ranges** panel opens when you select **gNodeB** from the RAN pane. It consists of two main section: Ranges and Ranges Connectivity.

### Ranges

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

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

### For example ...



## Ranges Connectivity

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

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

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

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

	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6
gNodeB-1						
gNodeB-2						
gNodeB-3						
gNodeB-4						
gNodeB-5						
gNodeB-6						

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.

The screenshot shows the 'Ranges Connectivity' interface. On the left, there's a list of 'RANGES' with checkboxes next to each entry. The entries are: Name: gNodeB-1 (checked), Name: gNodeB-2 (checked), Name: gNodeB-3 (checked), Name: gNodeB-4 (unchecked), Name: gNodeB-5 (checked), and Name: gNodeB-6 (checked). A red circle highlights the 'Name: gNodeB-4' entry. On the right is a 6x6 matrix representing connectivity between gNodeBs. The columns and rows are labeled gNodeB-1 through gNodeB-6. The matrix cells contain checkboxes. A red arrow points from the 'Name: gNodeB-4' entry in the list to the cell in the matrix where the checkbox is checked and circled in red.

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.

This screenshot shows the same interface after some changes. The 'Ranges' list now includes: Name: gNodeB-1 (checked), Name: gNodeB-2 (checked), Name: gNodeB-3 (unchecked), Name: gNodeB-4 (unchecked), Name: gNodeB-5 (checked), Name: gNodeB-6 (checked), and Name: gNodeB-7 (checked). In the matrix, the row for 'gNodeB-3' contains several checkboxes that are now greyed out, indicating they are disabled because their corresponding range is not selected.

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

<b>State</b>	<b>Description</b>	<b>Operation</b>
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.

The screenshot shows the 'Ranges Connectivity' panel. On the left, a sidebar lists 'RANGES' with checkboxes for seven gNodeB nodes: 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. On the right, a main table displays connectivity status for each gNodeB node across seven columns labeled gNodeB-1 through gNodeB-7. Each row has a header cell with a red circle and a switch icon. The first column's switch is highlighted with a red circle.

	gNodeB-1	gNodeB-2	gNodeB-3	gNodeB-4	gNodeB-5	gNodeB-6	gNodeB-7
gNodeB-1	On (highlighted)	Off	Off	Off	Off	Off	Off
gNodeB-2	Off	On	On	On	On	On	On
gNodeB-3	On	On	On	On	On	On	On
gNodeB-4	On	On	On	On	On	On	On
gNodeB-5	On	On	On	On	On	On	On
gNodeB-6	On	On	On	On	On	On	On
gNodeB-7	On	On	On	On	On	On	On

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 <b>Delete Range</b> 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.

Setting	Description
<i>Range Settings:</i>	
Node Settings	Each gNodeB range requires the configuration of an associated set of Node Settings, which are described in <a href="#">gNodeB node settings</a> .
NSSAI	Each gNodeB range requires the configuration of at least one NSSAI, and may specify multiple NSSAIs. These settings are described in <a href="#">gNodeB NSSAI settings</a> .
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 <a href="#">gNodeB N2 interface settings</a> .
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 <a href="#">gNodeB N3 interface settings</a> .

## 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	The S1AP connection timeout.

Setting	Description
Timeout (ms)	
Perform Load Balancing	Select the option to enable it. Performs load balancing between MMEs from the same MME group for initial attach.
Dynamic RAN UE NGAP/S1AP ID	If enabled, it will allocate dynamic RAN UE NGAP/S1AP ID values at Service Request.

## EPS Fallback Settings

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

The following parameters are required to configure the EPS fallback:

Setting	Description
Enable EPS Fallback	Select the check box to enable this option.
5QI	Select the 5G QoS identifier that will trigger the EPS fallback procedure. (The 5QI must be defined on the <a href="#">QoS Flow configuration settings on page 1016</a> panel in the <b>Global Settings</b> .)  When a request is received for this 5QI to create a dedicated QoS flow, the RAN will reject the request, which will trigger the EPS fallback procedure.
Associated ENB	Select the eNodeB used for handover.
Secondary Node	Select the secondary node from the drop-down list.  This option is used for EPS fallback to an eNodeB associated to a gNodeB using Option 3x.
EPS Fallback Mobility	Type of mobility to EPS during EPS fallback.  Select an option from the drop down list: <ul style="list-style-type: none"> <li>• <b>Handover to 4G</b></li> <li>• <b>Inter-System Redirection to 4G</b></li> </ul>
EPS Fallback Return Mobility	Type of mobility that occurs after the deletion of the dedicated bearer that triggered EPS fallback.  Select an option from the drop down list: <ul style="list-style-type: none"> <li>• <b>None</b> - After the dedicated bearer is deleted in 4G, the UE will not initiate any procedure.</li> <li>• <b>Connected Mode Handover to 5G</b> (default value) - After the</li> </ul>

Setting	Description
	<p>dedicated bearer is deleted in 4G, the UE will initiate a 4G to 5G Connected Mode Handover.</p> <ul style="list-style-type: none"> <li><b>Idle Mode Mobility to 5G</b> - 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.</li> </ul>
Send Service Request After EPS Fallback Return Mobility	<p>By default, this option is disabled.</p> <p>Send Service Request immediately after returning to 5G when Idle Mode Mobility to 5G was performed.</p>

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

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

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

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

Setting	Description
Public Warning System	Select the check box to enable this option.
PWS Restart Timer (s)	<p>Duration in seconds after which PWS Restart Indication is sent. The timer starts after the PWS Write-Replace message exchange. <b>0</b> indicates that no message is sent. For more details, refer to <i>TS 38.413 , 8.9.3 PWS Restart Indication</i>.</p> <p>Values should be in range 0-86400. Default value: <b>0</b>.</p>
PWS Failure Timer (s)	<p>Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. <b>0</b> indicates that no message is sent. For more details, refer to <i>TS 38.413 , 8.9.4 PWS Failure Indication</i>.</p> <p>Values should be in range 0-86400. Default value: <b>0</b>.</p>

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

## gNodeB NSSAI settings

Each UE range requires at least one NSSAI range.

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

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

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

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

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

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

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

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

## gNodeB N2 interface settings

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

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

By default, the N2 interface check box is enabled.

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

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

### N2 Interface Settings

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

Settings	Description
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.
SCTP Retry	<i>Select the check box to enable this option.</i>
Delay	The delay time (in milliseconds) for triggering a new SCTP retry, after a SCTP disconnect or a failed retry. For subsequent SCTP retries, consider the Connection Timeout value that will be added as well. Default value: <b>0</b> . Allowed integer value: minimum of 0.
Number of Retries	The maximum number of SCTP retries sent by RAN to reestablish the SCTP connection. Default value: <b>3</b> . Allowed integer value: minimum of 1.

## 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 <b>500</b> and cannot be changed.
Source Port	Set the source port number.
Enable NAT-T	Select to enable the NAT Traversal keepalive.
Inner IP Type	Select the IP type: <b>IPv4</b> or <b>IPv6</b> .
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to <b>Certificates</b> and cannot be changed.
CA Certificate	Select the <a href="#">CA certificate</a> 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 <b>Upload</b> button. To remove the archive , select the <b>Clear</b> button.</p> <p>The <code>.key</code> and <code>.crt</code> files need to have the same name before extensions.</p>

<b>Settings</b>	<b>Description</b>
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: <b>AES-128-GCM-16</b>. Available options: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b>.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: <b>NONE</b>. Available options: <b>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</b>.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> <li>• When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>• If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
DH Group	<p>Select an option from the drop-down list.</p> <p>Default value: <b>prime256v1(19)</b>. Available options: <b>prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32)</b>.</p>
PRF Algorithm	<p>Select an option from the drop-down list.</p> <p>Default value: <b>HMAC-SHA256</b>. Available options: <b>HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512</b>.</p>
<i>IKE Phase 2</i>	
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: <b>AES-128-GCM-16</b>. Available options: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b>.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: <b>NONE</b>. Available options: <b>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</b>.</p> <p>Restrictions:</p>

Settings	Description
	<ul style="list-style-type: none"> <li>When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list.</p> <p>Default value: <b>ID_DER ASN1 DN</b>. Available options: <b>ID_IPV4_ADDR</b>, <b>ID_FQDN</b>, <b>ID_USER_FQDN</b>, <b>ID_IPV6_ADDR</b>, <b>ID_DER ASN1 DN</b>, <b>ID_KEY_ID</b>.</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: <b>ID_FQDN</b>, <b>ID_KEY_ID</b> or <b>ID_RFC822_ADDR</b>.</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: <b>0</b> (disabled).</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>
DPD Interval (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>
<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).
Emulated Router Address	<p>Set the IPv4 or IPv6 address for the emulated router. This allows to hide all messages from the interface behind a MAC address.</p> <p><b>NOTE</b> This option can be used only with IxStack stack.</p>

Settings	Description
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 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID..

## 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	This option is available only if <a href="#">IPsec check box</a> 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

<b>Connectivity Settings</b>	<b>Description</b>
	required.
Peer SEG	Select the peer SEG range from the drop-down list.
Destination Port	By default, the destination port is set to <b>500</b> and cannot be changed.
Source Port	Set the source port number.
Enable NAT-T	Select to enable the NAT Traversal keepalive.
Inner IP Type	Select the IP type: <b>IPv4</b> or <b>IPv6</b> .
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to <b>Certificates</b> and cannot be changed.
CA Certificate	Select the <a href="#">CA certificate</a> 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 <b>Upload</b> button. To remove the archive , select the <b>Clear</b> button.</p> <p>The <b>.key</b> and <b>.crt</b> 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: <b>AES-128-GCM-16</b>. Available options: <b>AES-128-CBC</b>, <b>AES-192-CBC</b>, <b>AES-256-CBC</b>, <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b>, <b>AES-256-GCM-16</b>.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: <b>NONE</b>. Available options: <b>NONE</b>, <b>HMAC-MD5-96</b>, <b>HMAC-SHA1-96</b>, <b>HMAC-MD5-128</b>, <b>HMAC-SHA1-160</b>, <b>HMAC-SHA2-256-128</b>, <b>HMAC-SHA2-384-192</b>, <b>HMAC-SHA2-512-256</b>.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> <li>When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>

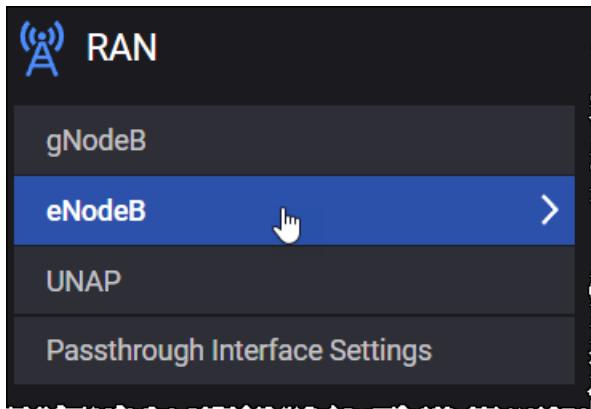
<b>Connectivity Settings</b>	<b>Description</b>
DH Group	Select an option from the drop-down list. Default value: <b>prime256v1(19)</b> . Available options: <b>prime256v1(19)</b> , <b>secp384r1(20)</b> , <b>secp521r1(21)</b> , <b>prime192v1(25)</b> , <b>secp224r1(26)</b> , <b>x25519(31)</b> , <b>x448(32)</b> .
PRF Algorithm	Select an option from the drop-down list. Default value: <b>HMAC-SHA256</b> . Available options: <b>HMAC-MD5</b> , <b>HMAC-SHA1</b> , <b>HMAC-SHA256</b> , <b>HMAC-SHA384</b> , <b>HMAC-SHA512</b> .
<i>IKE Phase 2</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: <b>AES-128-GCM-16</b> . Available options: <b>AES-128-CBC</b> , <b>AES-192-CBC</b> , <b>AES-256-CBC</b> , <b>AES-128-GCM-16</b> , <b>AES-192-GCM-16</b> , <b>AES-256-GCM-16</b> .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: <b>NONE</b> . Available options: <b>NONE</b> , <b>HMAC-MD5-96</b> , <b>HMAC-SHA1-96</b> , <b>HMAC-MD5-128</b> , <b>HMAC-SHA1-160</b> , <b>HMAC-SHA2-256-128</b> , <b>HMAC-SHA2-384-192</b> , <b>HMAC-SHA2-512-256</b> . Restrictions: <ul style="list-style-type: none"> <li>• When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>• If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
<i>Identification</i>	
Local Identification Type	Select an option from the drop-down list. Default value: <b>ID_DER ASN1 DN</b> . Available options: <b>ID_IPV4_ADDR</b> , <b>ID_FQDN</b> , <b>ID_USER_FQDN</b> , <b>ID_IPV6_ADDR</b> , <b>ID_DER ASN1 DN</b> , <b>ID_KEY_ID</b> .
Local Identification Value	Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: <b>ID_FQDN</b> , <b>ID_KEY_ID</b> or <b>ID_RFC822_ADDR</b> .
<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: <b>0</b> (disabled).

<b>Connectivity Settings</b>	<b>Description</b>
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: <b>0</b> (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: <b>0</b> (disabled).
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
Emulated Router Address	Set the IPv4 or IPv6 address for the emulated router. This allows to hide all messages from the interface behind a MAC address.  <div style="border: 1px solid #ccc; padding: 5px; display: inline-block;">NOTE</div> 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>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

Connectivity Settings	Description
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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..

## 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:

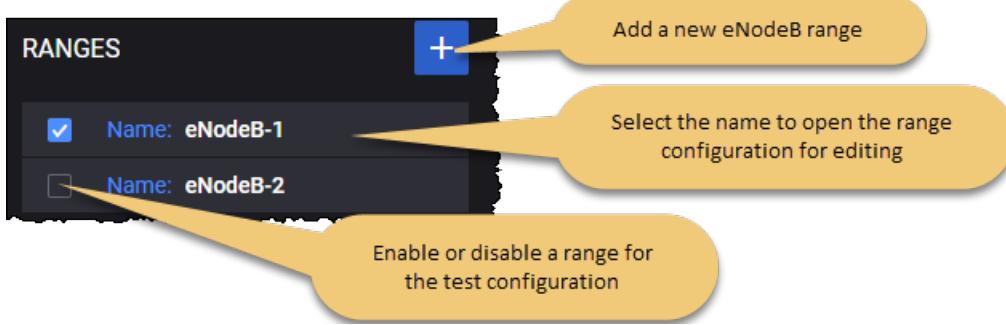
<b>eNodeB Ranges panel</b> .....	<b>1180</b>
<b>eNodeB Range Settings</b> .....	<b>1184</b>
<b>eNodeB Node Settings</b> .....	<b>1185</b>
<b>S1-U Interface Settings</b> .....	<b>1186</b>
<b>S1-MME Interface Settings</b> .....	<b>1187</b>

### 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:

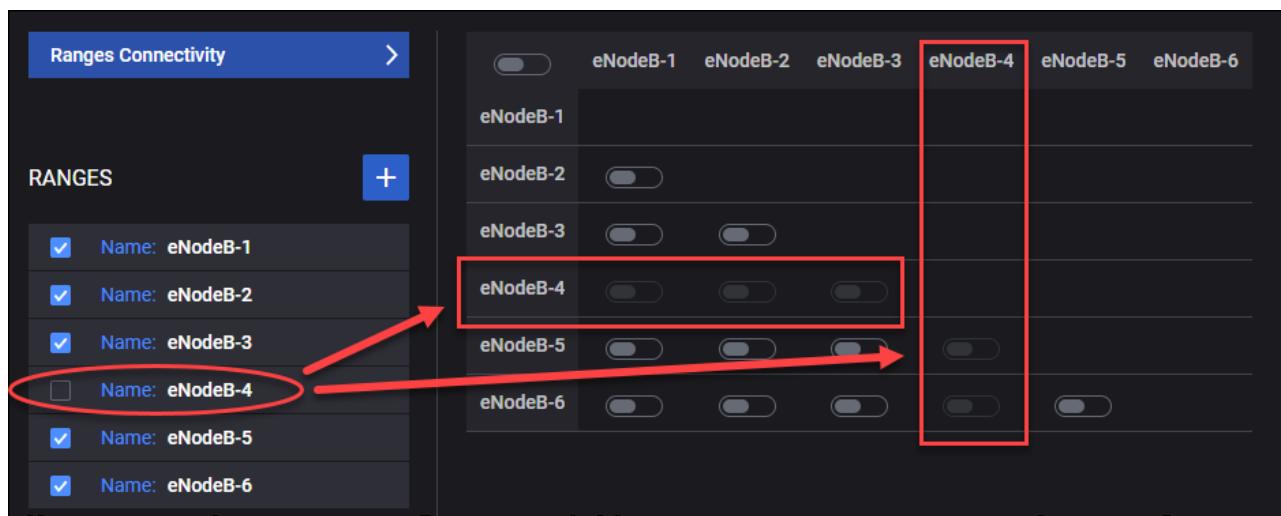
State	Description
Selected and blue color	An X2 link connection is established between enabled eNodeB ranges.
Selected and grey color	An X2 link connection is established between disabled eNodeB ranges.
Unselected	No X2 link connection between eNodeB ranges.

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.



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.

	eNodeB-1	eNodeB-2	eNodeB-3	eNodeB-4	eNodeB-5	eNodeB-6
eNodeB-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-3	<input type="checkbox"/>	<input type="checkbox"/>	<input 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 checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

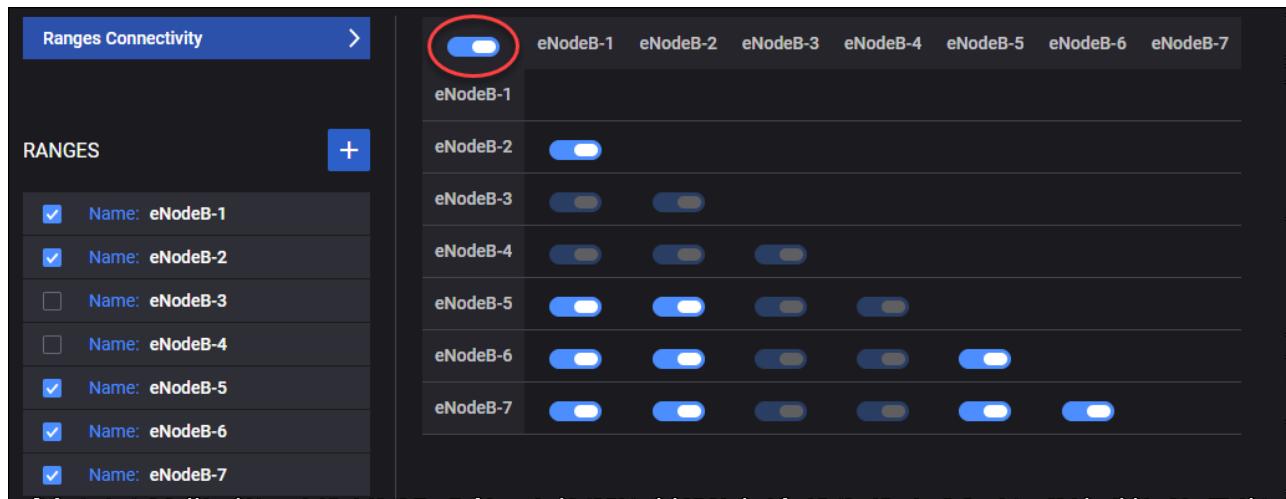
2. The eNodeB-3 range was enabled on previous step and there were selected X2 links between eNodeB-3/eNodeB-4 and eNodeB-3/eNodeB-6. Due to the fact that eNodeB-3 is now disabled, the check-box for X2 links between eNodeB-3 and eNodeB-6 have become greyed out.

	eNodeB-1	eNodeB-2	eNodeB-3	eNodeB-4	eNodeB-5	eNodeB-6	eNodeB-7
eNodeB-1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-5	<input checked="" type="checkbox"/>	<input type="checkbox"/>					
eNodeB-6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
eNodeB-7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The first cell of matrix contains a main check-box that displays the state of the matrix and perform operations.

State	Description	Operation
Selected	All connected.	If the main check-box is Selected, you can undo the selection to change the state to Unselected and all X2 links from the connectivity matrix will become unselected (none connected).
Unselected	None connected.	If the main check-box is Unselected, you can select it to change the state to Checked and all X2 links from the connectivity matrix will become selected (all connected).

When the main matrix check-box is selected all the X2 link check-boxes from the matrix become selected.



Even the X2 link check-boxes for disabled eNodeB ranges are selected since the X2 links for disabled eNodeB ranges are not sent to the traffic agent. This way, when the disabled eNodeB range is enabled, you will not have to manually select the X2 link check-boxes for that particular eNodeB range.

## eNodeB Range Settings

Each eNodeB range is identified by a unique name. You can add and delete ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each eNodeB range.

Setting	Description
<i>Range:</i>	
	Select the <b>Delete Range</b> 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 <a href="#">eNodeB node settings</a> .
S1-U Interface Settings	Each eNodeB range requires the configuration of an associated set of S1-U Interface Settings, which are described in <a href="#">S1-U interface settings</a> .
S1-MME Interface Settings	Each eNodeB range requires the configuration of an associated set of S1 Interface Settings, which are described in <a href="#">S1-MME interface settings</a> .

## 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.
Dynamic RAN UE NGAP/S1AP ID	If enabled, it will allocate dynamic RAN UE NGAP/S1AP ID values at Service Request.

The following parameters are required under the **Public Warning System** pane:

Setting	Description
Public Warning System	Select the check box to enable this option.
PWS	Duration in seconds after which PWS Restart Indication is sent. The timer starts after

Setting	Description
Restart Timer (s)	the PWS Write-Replace message exchange. <b>0</b> indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.3 PWS Restart Indication</i> . Values should be in range 0-86400. Default value: <b>0</b> .
PWS Failure Timer (s)	Duration in seconds after which PWS Failure Indication is sent. The timer starts after the PWS Write-Replace message exchange. <b>0</b> indicates that no message is sent. For more details, refer to <i>TS 38.413, 8.9.4 PWS Failure Indication</i> . Values should be in range 0-86400. Default value: <b>0</b> .

**NOTE** If the *Public Warning System* option is enabled and both PWS Restart and PWS Failure procedures are configured to be initiated (non-zero timers), the timers should be different.

## S1-U Interface Settings

The **S1-U Interface Settings** should be enabled and configured when the test is simulating the MME and the DUT is an SGW. When LoadCore simulates the MME and the SGW, these settings should be disabled.

In 4G networks, S1-U is the reference point between the LTE eNodeB and the LTE S-GW. It uses the GTP-U protocol running on top of UDP to provides best-effort data delivery of user datagrams. One GTP tunnel is established for each radio bearer to carry user traffic between the eNodeB and the selected SGW.

## Connectivity Settings

**NOTE** The following connectivity settings are available in LoadCore Web interface, but some of them can be configured only when DPDK is activated.

Connectivity Settings	Description
IP	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).
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.
	<b>NOTE</b> This option can be used only with IxStack stack.

Connectivity Settings	Description
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	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## 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.

<b>S1-MME Interface Settings</b>	<b>Description</b>
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.
<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.
SCTP Retry	<i>Select the check box to enable this option.</i>
Delay	The delay time (in milliseconds) for triggering a new SCTP retry, after a SCTP disconnect or a failed retry. For subsequent SCTP retries, consider the Connection Timeout value that will be added as well.

S1-MME Interface Settings	Description
	Default value: <b>0</b> . Allowed integer value: minimum of 0.
Number of Retries	The maximum number of SCTP retries sent by RAN to reestablish the SCTP connection. Default value: <b>3</b> . Allowed integer value: minimum of 1.

## Connectivity Settings

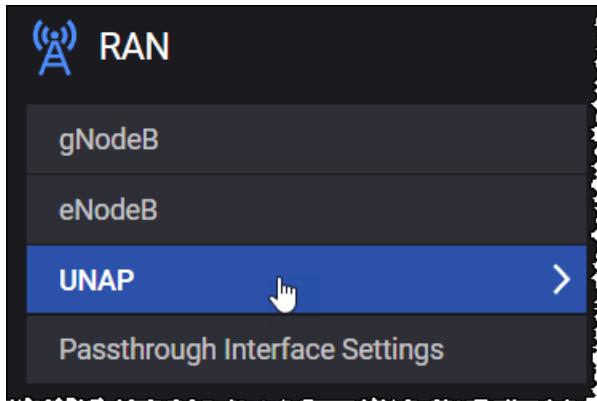
The following table describes the parameters that you need to configure for the connectivity settings:

Connectivity Settings	Description
<i>IP</i>	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address in your test network to use for traffic on this interface. If the <i>Range Count</i> is greater than 1, then this IP Address value is assigned to the first range and is incremented by 1 for each additional range.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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 <i>MAC Address</i> ). The default value is 000000000001.
Outer VLAN	Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

Connectivity Settings	Description
Inner VLAN	<b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

## UNAP

To configure one or more UNAP ranges for a test, select **UNAP** from the RAN panel.



The following topics describe the UNAP configuration settings:

**UNAP Ranges panel** ..... **1190**

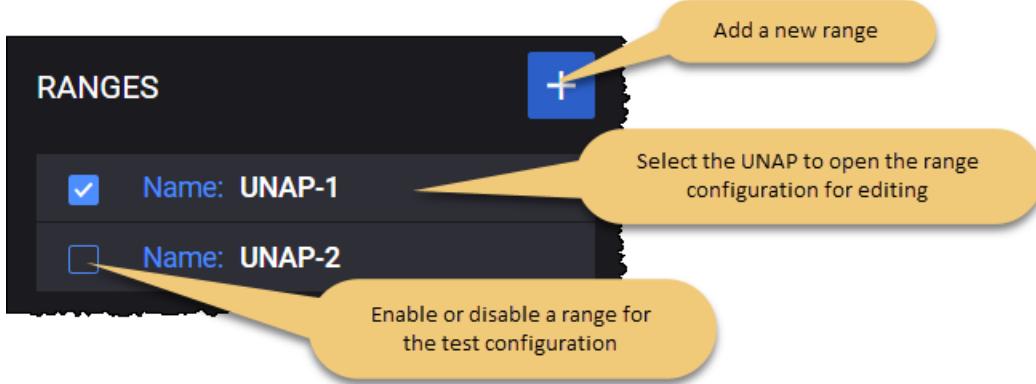
**UNAP Range Settings** ..... **1191**

### UNAP Ranges panel

The **UNAP Ranges** panel opens when you select the **UNAP** node from the **RAN** pane. On the Ranges panel, you can perform the following task:

- Add a new UNAP range to your test configuration.
- Open a UNAP range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



## UNAP Range Settings

Each UNAP range is identified by a unique name. You can add and delete ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each UNAP range.

Setting	Description
<i>Range:</i>	
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
Range Count	Enter the number of simulated UNAPs required for the range. Default value is <b>1</b> .
<i>Range Settings:</i>	
<i>Node Settings</i>	<i>Each UNAP range requires the configuration of an associated set of Node Settings.</i>
Name	<p>The name of this UNAP range. Multiple UNAP instances (ranges) may be deployed in the test network.</p> <p>Each UNAP instance is uniquely identified by its name. You can accept the value provided by LoadCore or overwrite it with your own value.</p>
UNAP ID	Provide the UNAP identifier value.
UNAP ID Increment	Set the UNAP identifier increment value.
<i>WLAN IP Pool</i>	<i>Each UNAP range requires connectivity settings configuration, which is described in the <a href="#">Connectivity Settings table</a>.</i>

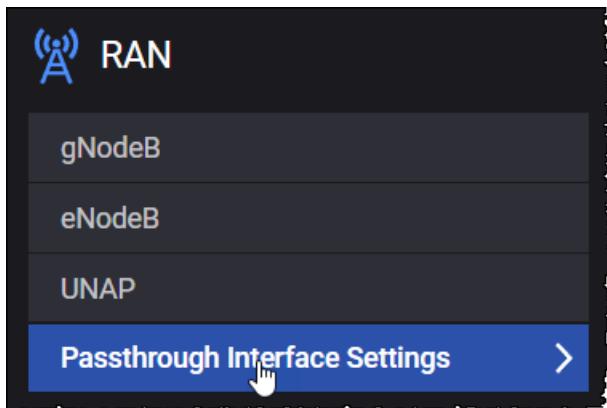
## Connectivity Settings

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
IP Address Increment	Set the IP address increment value.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.
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.
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 0.0.0.1.
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.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## 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: <b>Single Stack</b> or <b>Dual Stack</b> .
IP	<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.

<b>Connectivity Settings</b>	<b>Description</b>
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 <b>Dual Stack</b>.</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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>

<b>Connectivity Settings</b>	<b>Description</b>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## SEG/N3IWF & Core configuration settings

The configuration settings are described in the topics listed below.

### Topics:

<b>Core settings</b> .....	<b>1195</b>
<b>N6/SGi interface settings</b> .....	<b>1197</b>
<b>Core Ranges settings</b> .....	<b>1198</b>
AMF Ranges configuration settings .....	1198
UPF Ranges configuration settings .....	1208
MME Ranges configuration settings .....	1210
SGW Ranges configuration settings .....	1219
<b>SEG Ranges configuration settings</b> .....	<b>1222</b>
SEG interface settings .....	1226
<b>N3IWF Ranges configuration settings</b> .....	<b>1226</b>
N3IWF interface settings .....	1233

If multiple agents are assigned to the SEG/N3IWF topology, the **Distribution Mode** parameter (see [Distribution Mode feature on page 69](#)) is displayed and the following options can be selected from the drop-down:

- **All Ranges on All Agents** - influences the way configuration is distributed in case of multiple agents assigned on the SEG/N3IWF node.  
For example, for a test with 2 agents and 3 ranges: range1 on agent1 and agent2, range2 on agent1 and agent2, range3 on agent1 and agent2.

## 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.

<b>Setting</b>	<b>Description</b>
Home Network Private Key	The Home Network Private key that is used for subscriber privacy.

<b>Setting</b>	<b>Description</b>
<i>Routing Indicators</i>	<p><i>The Routing Indicator is used in combination with the MCC and MNC to route network signaling to AUSF and UDM instances that are capable of serving the subscriber. It contains four decimal digits, is assigned by the home network operator, and provisioned in the USIM.</i></p> <p><i>You can add as many Routing Indicators as necessary to support your test objectives.</i></p>
	Select the <b>Add Routing Indicator</b> button to add a Routing Indicator.
	Select the <b>Delete</b> button to remove the routing indicator.
<i>PCRF Node Settings</i>	<p><b>NOTE</b> <i>These settings are available only when Core is set as DUT (for more details, refer to <a href="#">Core Ranges settings</a>.)</i></p> <p><i>You can enable or disable the PCRF Node Settings, as required by your test configuration.</i></p>
<i>Origin Host Prefix</i>	Set the origin host prefix. Default value: <b>host</b> .
<i>Origin Realm</i>	Set the origin realm. Default value: <b>keysight.com</b> .
<i>Rx Interface Settings</i>	<p><i>The Rx Interface Settings panel is available only when the <a href="#">PCRF Node Settings</a> panel is enabled.</i></p> <p><i>The Rx interface settings are described <a href="#">below</a>.</i></p>

## Rx Interface Settings

<b>Connectivity Settings</b>	<b>Description</b>
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
<i>IP Address</i>	The IP address from your test network to use for traffic on this interface.
<i>IP Prefix Length</i>	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>Gateway Address</i>	The IP address assigned as gateway address.
<i>Gateway Increment</i>	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>Port</i>	The port number to use for this interface communications. The default is port 3868, but you can choose a different port number.

## N6/SGi interface settings

N6 is the interface between the UPF session anchor and the DN. It is the interconnection point at which user plane packet encapsulation and decapsulation is performed.

The following **Connectivity Settings** enable the necessary N6/SGi connectivity and service interaction.

Connectivity Settings	Description
Stack Type	Select the stack type from the drop-down list. Available options: <b>Single Stack</b> or <b>Dual Stack</b> .
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	Maximum transmission unit.
MSS	Maximum segment size.
<i>Secondary IP</i>	<i>Select the IP address to open the secondary IP configuration panel for editing. This panel is available only when the stack type is set to <b>Dual Stack</b>.</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 MAC

<b>Connectivity Settings</b>	<b>Description</b>
	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><b>IMPORTANT</b> This option is visible only when the Outer VLAN 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.

## Core Ranges settings

When you select the Core Ranges pane ,LoadCore opens the Core Range panel, from which you can:

- Designate the range as a **Device Under Test**.
- Select the corresponding pane to configure the core range and connectivity settings:
  - [AMF Ranges](#)
  - [UPF Ranges](#)
  - [MME Ranges](#)
  - [SGW Ranges](#)

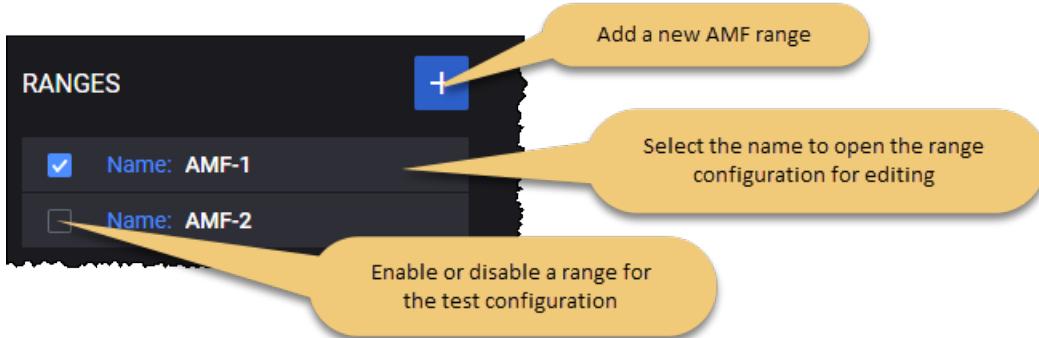
### AMF Ranges configuration settings

To access and configure the AMF ranges settings, select **AMF Ranges** from the Core Ranges panel.

You can perform the following tasks from the **Ranges** panel:

- Add a new AMF range to your test configuration.
- Open an AMF range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



You add and select AMF ranges from the Ranges panel. When you select the name of an AMF, 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 <b>Delete Range</b> 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 <a href="#">AMF node settings</a> .
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 <a href="#">AMF N2 interface settings</a> .

### AMF node settings

Each AMF range includes a set of Node Settings.

#### Node Settings

Each AMF instance (that is, each range) is identified by the following node settings.

Setting	Description
<i>Node Settings:</i>	
Instance ID	Multiple AMF instances may be deployed in the 5G network.

<b>Setting</b>	<b>Description</b>
	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.
Name	The name uniquely identifies each AMF instance. 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><b>About PLMN MCC ...</b></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><b>About PLMN MNC ...</b></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 identifies the AMF Set within the AMF Region.</p>
Pointer	The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.
Relative Capacity	Set the relative capacity value.
Ciphering Algorithm	<p>Allows to select the supported 5G ciphering algorithm:</p> <ul style="list-style-type: none"> <li>• NEA0 - Null ciphering algorithm</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>NEA1 - 128-bit SNOW 3G based algorithm</li> <li>NEA2 - 128-bit AES based algorithm</li> <li>NEA3 - 128-bit ZUC based algorithm</li> </ul>
Integrity Algorithm	Allows to select the supported 5G integrity protection algorithm: <ul style="list-style-type: none"> <li>NIA0 - Null Integrity Protection algorithm</li> <li>NIA1 - 128-bit SNOW 3G based algorithm</li> <li>NIA2 - 128-bit AES based algorithm</li> <li>NIA3 - 128-bit ZUC based algorithm</li> </ul>
Request N2 SM Information	Enable this option to request N2 SM Information again instead of using the existing one.
Prefer AMF Change	Enable this option to change the AMF for an N2 handover even when the target RAN(T-RAN) is connected to the serving AMF.
Skip MT SMS	If enabled, it will skip the initiation of the MT SMS procedure when the MO SMS procedure ends.

*T3512: Select the check box to open T3512 Settings and configure the T3512 timer.*

**NOTE**

*If disabled, a value of 50 minutes (Value 5 X Unit 10 minutes) is sent for T3512.*

Value	Set the value for this parameter. The accepted values are between 0-31.
Unit	Select the unit size for this parameter from the drop-down list. The available options are: 2s, 30s, 1m, 10m, 1h, 10h and Deactivated.
NSSAI	<i>These settings are described <a href="#">below</a>.</i>
TAI	<i>These settings are described <a href="#">below</a>.</i>
Public Warning System	<i>These settings are described <a href="#">below</a>.</i>
AMF Configuration Update	<i>AMF Configuration Updates can modify AMF name, AMF Relative Capacity, or the Supplementary GUAMI and PLMN List. After an AMF Configuration Update procedure, the newly advertised values are not applied further in the test.</i> <i>These settings are described <a href="#">below</a>.</i>
Emergency Settings	<i>These settings are described <a href="#">below</a>.</i>
Overload Configuration	<i>Select the check box to enable this option. This option allows you to configure the 4G and 5G overload.</i>
Delay	The time to wait (in seconds), to send the Overload Start after each successful

Setting	Description
	S1 Setup. A <b>0</b> value means the procedure is not initiated.
Duration	The duration of the overload, in seconds, after which the Overload Stop is sent.
Overload Action	Select the overload action to be taken: <ul style="list-style-type: none"> <li>• <b>None</b> (default) - means the action is not taken</li> <li>• <b>Reject RRC connection establishments for non-emergency MO DT</b></li> <li>• <b>Reject RRC connection establishments for Signalling</b></li> <li>• <b>Permit Emergency Sessions and mobile terminated services only</b></li> <li>• <b>Permit High Priority Sessions and mobile terminated services only</b></li> </ul>
Traffic Load Reduction Indication	This option may be included only if the overload action is present. A <b>0</b> value indicates the IE will not be included.
Reset Configuration	<i>Select the check box to enable this option.</i>
Delay (s)	Time to wait, in seconds, to initiate the NG Reset procedure after the NG Setup was performed. The reset is scheduled for each NG RAN connection.

## NSSAI

The following table describes the configuration settings that are required for NSSAI.

Setting	Description												
<b>NSSAI:</b>													
	Select the Add NSSAI button to add a new NSSAI to your test configuration.												
<b>NSSAI settings:</b>													
	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											

Setting	Description
SD	The Slice Differentiator (SD) value for this S-NSSAI. SD is an optional information that differentiates amongst multiple Network Slices of the same Slice/Service type. The SD field comprises octets 4 through 6 in the NSSAI.

## TAI

The following table describes the configuration settings that are required for TAI.

Setting	Description
<i>TAI:</i>	
	Select the Add TAI button to add a new TAI (Tracking Area Identity) to your test configuration.
<i>TAI settings:</i>	
	Select the Delete TAI button to delete this TAI from your test configuration.
<i>PLMN ID:</i> Set the values for the PLMN identifier.	
PLMN MCC	The PLMN Mobile Country Code (MCC) used in the construction of the TAI.
PLMN MNC	The PLMN Mobile Network Code (MNC) used in the construction of the TAI.
<i>TAC:</i>	
	Select the Add TAC button to add a new TAC (Tracking Area Code) to your test configuration.
<i>Settings:</i>	
	Select the Delete TAC button to delete this TAC from your test configuration.
TAC	The Tracking Area Code (TAC) used in the construction of the TAI.

## Public Warning System

The following table describes the configuration settings that are required for public warning system.

Setting	Description
Message ID	Set the public warning system message ID.
Repetition Period	Set the public warning system message repetition period.
Number of Broadcasts Requested	Set the public warning system message number of requested broadcasts.

Setting	Description
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.
Write Replace Warning Area List	Select one of the drop-down options to configure the areas where the warning message needs to be broadcast: <ul style="list-style-type: none"> <li>• <b>None</b> (default), the Warning Area List IE will be omitted.</li> <li>• <b>TAI List</b>- this enables the <b>TAI List</b> parameter, to add the TAIs that will receive the warnings; refer to <a href="#">TAI</a> table above for the configuration of Tracking Area Identities required.</li> <li>• <b>NR Cell ID List</b>- this enables the <b>NR Cell ID List</b> parameter, to add the NR Cell IDs that will receive the warnings; refer to <a href="#">NR Cell ID List</a> table below for further configuration.</li> </ul>
Cancel Warning Area List	Select one of the drop-down options to configure the areas where the warning message needs to be canceled: <ul style="list-style-type: none"> <li>• <b>None</b> (default), the Warning Area List IE will be omitted.</li> <li>• <b>TAI List</b>- this enables the <b>TAI List</b> parameter, to add the TAIs that will receive the PWS cancel; refer to <a href="#">TAI</a> table above for the configuration of Tracking Area Identities required.</li> <li>• <b>NR Cell ID List</b>- this enables the <b>NR Cell ID List</b> parameter, to add the NR Cell IDs that receive the PWS cancel; refer to <a href="#">NR Cell ID List</a> table below for further configuration.</li> </ul>
Popup	If enabled, it will activate a pop-up on the UE when receiving an ETWS message.
Emergency User Alert	If enabled, it will activate the emergency user alert on the UE when receiving an ETWS message.
Data coding scheme	Select an option from the drop-down to set the data coding scheme for PWS/ETWS messages.
Warning Message Contents	Add the content of the warning message that will be broadcasted to the UEs.

### NR Cell ID List

The following table describes the configuration settings that are required for NR Cell ID.

Setting	Description
<i>NR Cell ID:</i>	

Setting	Description
	Select the Add NR Cell ID button to add a new UE ID to your test configuration.
<i>NR Cell ID settings:</i>	
	Select the Delete NR Cell ID button to delete this UE ID 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 NR Cell ID.
PLMN MNC	The PLMN Mobile Network Code (MNC) used in the construction of the NR Cell ID.
NR Cell ID	The cell identifier of the UE.

### AMF Configuration Update(s)

The following table describes the configuration settings that are required for AMF Configuration Update.

Setting	Description
<i>AMF Configuration Update(s):</i>	
	Select the Add AMF Configuration Update(s) button to configure a new AMF Configuration Update message.
<i>AMF Configuration Update:</i>	
	Select the Delete AMF Configuration Update button to delete the AMF Configuration Update message configuration.
Delay (ms)	The delay between NG setup and the first AMF Configuration Update, or between subsequent AMF Configuration Update procedures.
<i>Updated Item(s):</i>	
	Select the Add Updated Item button to add a new item to be updated.
<i>Updated Item:</i>	
	Select the Delete Updated Item button to delete this item from your test configuration.
Type	Select one of the update options: <ul style="list-style-type: none"> <li>• <b>Updated AMF Name</b> - refers to the AMF instance name (see <b>Value</b>)</li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• <b>Updated Relative Capacity</b> - refers to the AMF instance relative capacity (see <b>Value</b>)</li> <li>• <b>Supplementary GUAMI</b> - AMF Configuration Update messages for Supplementary GUAMI/PLMN Support List always include the GUAMI/PLMN Support List original values (at NG setup), besides the ones in the update, to avoid impact on the current test.</li> </ul>
<b>Value</b>	<p>If <b>Type</b> is set as:</p> <ul style="list-style-type: none"> <li>• <b>Updated AMF Name</b> - it will allow you to update the unique name that identifies the selected AMF instance.</li> <li>• <b>Updated Relative Capacity</b> - will allow to update the relative capacity value, which should be between 0 and 255.</li> </ul>
<b>MCC</b>	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUAMI</b>.</p> <p>The MCC for this AMF range.</p>
<b>MNC</b>	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUAMI</b>.</p> <p>The MNC for this AMF range.</p>
<b>Region ID</b>	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUAMI</b>.</p> <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>
<b>Set ID</b>	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUAMI</b>.</p> <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>
<b>Pointer</b>	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUAMI</b>.</p> <p>The AMF Pointer to use for this simulated AMF node. The AMF Pointer identifies one or more AMFs within the AMF Set.</p>

## Emergency Settings

The following table describes the emergency settings configuration.

<b>Setting</b>	<b>Description</b>
Authentication Behaviour	<p>The authentication procedure behaviour during an Emergency Registration.</p> <p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Normal Authentication (default value)</li> <li>• Allow Authentication Failure</li> <li>• Skip Authentication</li> </ul>
Emergency Services Support Value	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Not Supported (default value)</li> <li>• In NR connected to 5GC only</li> <li>• In EUTRA connected to 5GC only</li> <li>• In NR connected to 5GC and EUTRA connected to 5GC</li> </ul>
Emergency Services Fallback Support Value	<p>Select an option from the drop-down list:</p> <ul style="list-style-type: none"> <li>• Not Supported (default value)</li> <li>• In NR connected to 5GC only</li> <li>• In EUTRA connected to 5GC only</li> <li>• In NR connected to 5GC and EUTRA connected to 5GC</li> </ul>

## 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.

<b>Connectivity Settings</b>	<b>Description</b>
<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>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>

<b>Connectivity Settings</b>	<b>Description</b>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route from your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.

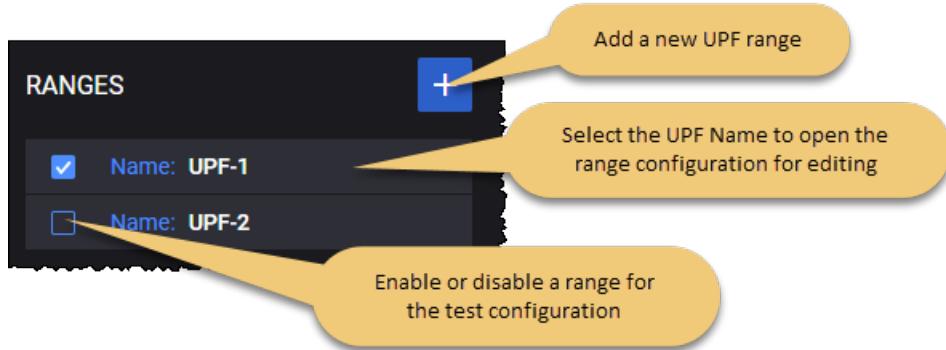
## UPF Ranges configuration settings

To access and configure the UPF ranges settings, select **UPF Ranges** from the Core Ranges panel.

You can perform the following tasks from the **Ranges** panel:

- Add a new UPF range to your test configuration.
- Open a UPF range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



You add and select UPF ranges from the Ranges panel. When you select an UPF range *Name*, 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 <b>Delete Range</b> 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 <a href="#">UPF N3 interface settings</a> .

## UPF N3 interface settings

The following configuration settings are required by each UPF N3 range.

Connectivity Settings	Description
IP	Select the IP address to open the IP configuration panel for editing.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.

<b>Connectivity Settings</b>	<b>Description</b>
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
MTU	Maximum transmission unit.
MSS	Maximum segment size.
Additional Routes	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route from your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the MAC Address). The default value is 000000000001.
Outer VLAN	<i>Select the check-box to make this option available, and, then, select the Outer VLAN to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

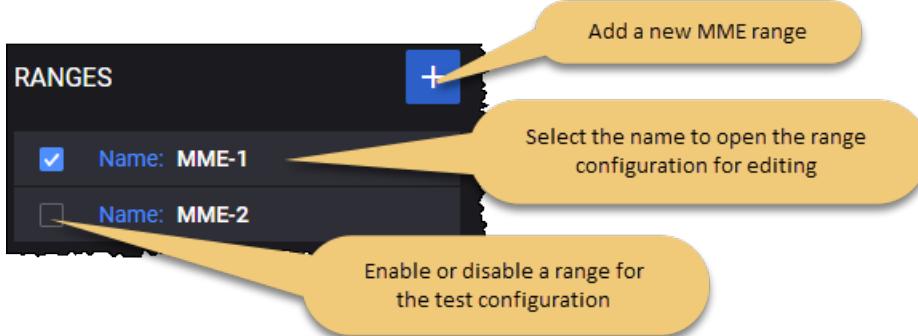
## MME Ranges configuration settings

To access and configure the MME ranges settings, select **MME Ranges** from the Core Ranges panel.

You can perform the following tasks from the **Ranges** panel:

- Add a new MME range to your test configuration.
- Open an MME range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

### For example ...



You add and select MME ranges from the MME Ranges panel. When you select the name of an MME , 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
<i>Range:</i>	
	Select the <b>Delete Range</b> 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 <a href="#">MME node settings</a> .
S1 Interface Settings	These settings are described in <a href="#">MME S1 interface settings</a> .

## 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><b>About PLMN MCC ...</b></p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this MME range.</p> <p><b>About PLMN MNC ...</b></p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Ciphering Algorithm	<p>Allows to select the supported 5G ciphering algorithm:</p> <ul style="list-style-type: none"> <li>• <b>EEA0</b> - Null ciphering algorithm</li> <li>• <b>EEA1</b> - 128-bit SNOW 3G based algorithm</li> <li>• <b>EEA2</b> - 128-bit AES based algorithm</li> <li>• <b>EEA3</b> - 128-bit ZUC based algorithm</li> </ul>
Integrity Algorithm	<p>Allows to select the supported 5G integrity protection algorithm:</p> <ul style="list-style-type: none"> <li>• <b>EIA0</b> - Null Integrity Protection algorithm</li> <li>• <b>EIA1</b> - 128-bit SNOW 3G based algorithm</li> </ul>

<b>Setting</b>	<b>Description</b>
	<ul style="list-style-type: none"> <li>• <b>EIA2</b> - 128-bit AES based algorithm</li> <li>• <b>EIA3</b> - 128-bit ZUC based algorithm</li> </ul>
Relative Capacity	Set the relative capacity value.
<i>Public Warning System</i>	<i>Select the check box to enable this option.</i>
Message ID	Set the public warning system message ID. Values should be in range 0-65535. Default value: <b>4352</b> .
Repetition Period	Set the public warning system message repetition period. Values should be in range 1-131071. Default value: <b>1</b> .
Number of Broadcasts Requested	Set the public warning system message number of requested broadcasts. Values should be in range 0-65535. Default value: <b>1</b> .
Time to Wait Before Triggering PWS after NG Setup (s)	Set the number of seconds to wait before triggering PWS after S1 setup. Values should be in range 0-86400. Default value: <b>1</b> .
PWS Kill Timer (s)	Duration in seconds after which PWS Kill Request is sent. Values should be in range 0-86400. Default value: <b>0</b> .
Write Replace Warning Area List	Select one of the drop-down options to configure the areas where the warning message needs to be broadcast: <ul style="list-style-type: none"> <li>• <b>None</b> (default), the Warning Area List IE will be omitted.</li> <li>• <b>TAI List</b>- this enables the <b>TAI List</b> parameter, to add the TAIs that will receive the warnings; refer to <a href="#">TAI</a> table below for the configuration of Tracking Area Identities required.</li> <li>• <b>Cell ID List</b>- this enables the <b>Cell ID List</b> parameter, to add the Cell IDs that will receive the warnings; refer to <a href="#">Cell ID List</a> table below for further configuration.</li> </ul>
Kill Warning Area List	Select one of the drop-down options to configure the areas where the warning message needs to be killed: <ul style="list-style-type: none"> <li>• <b>None</b> (default), the Warning Area List IE will be omitted.</li> <li>• <b>TAI List</b>- this enables the <b>TAI List</b> parameter, to add the TAIs that will receive the PWS kill; refer to <a href="#">TAI</a> table below for the configuration of Tracking Area Identities required.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li><b>Cell ID List</b>- this enables the <b>Cell ID List</b> parameter, to add the Cell IDs that will receive the PWS kill; refer to <a href="#">Cell ID List</a> table below for further configuration.</li> </ul>
Popup	If enabled, it will activate a pop-up on the UE when receiving an ETWS message.
Emergency User Alert	If enabled, it will activate the emergency user alert on the UE when receiving an ETWS message.
Data coding scheme	Select an option from the drop-down to set the data coding scheme for PWS/ETWS messages.
Warning Message Contents	Add the content of the warning message that will be broadcasted to the UEs.
T3412	<p>Select the check box to enable this option.</p> <p><b>NOTE</b> <i>If enabled, it allows the configuration of the T3412 timer. If disabled, a value of 50 minutes (Value 5 x Unit 10 minutes) is sent for T3412.</i></p>
Value	Set the value for this parameter. Accepted values are between <b>0</b> and <b>31</b> .
Unit	<p>Select from the drop-down the unit to use for T3412 timer calculation. Supported values are:</p> <ul style="list-style-type: none"> <li>if <i>Support Extended Timer</i> is <b>enabled</b>, units are <b>2 seconds</b>, <b>30 seconds</b>, <b>1 minute</b>, <b>10 minutes</b>, <b>1 hour</b>, <b>10 hours</b>, <b>Deactivated</b>.</li> <li>if <i>Support Extended Timer</i> is <b>disabled</b>, units are <b>2 seconds</b>, <b>1 minute</b>, <b>10 hours</b>, <b>Deactivated</b>.</li> </ul>
Support Extended Time	If enabled (default), it sets the T3412 extended value as described in the TS 24.301, chapter 8.2.1.12.
MME Configuration Update	<p><i>MME Configuration Updates can modify MME name, MME Relative Capacity, or the Supplementary GUMMEI List. After an MME Configuration Update procedure, the newly advertised values are not applied further in the test.</i></p> <p><i>These settings are described <a href="#">below</a>.</i></p>
Emergency Settings	<i>This option allows you to configure the Emergency support and MME behavior for Authentication procedure.</i>
Allow Emergency Attach	This parameter is enabled by default; the MME will allow the UEs to use emergency attach.
Authentication Behaviour	Select one of the following behaviors to apply during Emergency Registration: <ul style="list-style-type: none"> <li><b>Normal Authentication</b></li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>• <b>Allow Authentication Failure</b></li> <li>• <b>Skip Authentication</b></li> </ul>
Overload Configuration	Select the check box to enable this option. This option allows you to configure the 4G and 5G overload.
Delay	The time to wait (in seconds), to send the Overload Start after each successful S1 Setup. A <b>0</b> value means the procedure is not initiated.
Duration	The duration of the overload, in seconds, after which the Overload Stop is sent.
Overload Action	Select the overload action to be taken: <ul style="list-style-type: none"> <li>• <b>Reject RRC connection establishments for non-emergency MO DT</b> (default)</li> <li>• <b>Reject RRC connection establishments for Signalling</b></li> <li>• <b>Permit Emergency Sessions and mobile terminated services only</b></li> <li>• <b>Permit High Priority Sessions and mobile terminated services only</b></li> <li>• <b>Reject delay tolerant access</b></li> <li>• <b>Permit high priority sessions and exception reporting and mobile terminated services only</b></li> <li>• <b>Not accept mo-data or delay tolerant access from CP CIoT</b></li> </ul>
Traffic Load Reduction Indication	This option may be included only if the overload action is present. A <b>0</b> value indicates the IE will not be included.
Reset Configuration	Select the check box to enable this option.
Delay (s)	Time to wait, in seconds, to initiate the S1 Reset procedure after the S1 Setup was performed. The reset is scheduled for each S1 RAN connection.

## TAI

The following table describes the configuration settings that are required for TAI.

Setting	Description
TAI:	
	Select the Add TAI button to add a new TAI (Tracking Area Identity) to your test configuration.
TAI settings:	

<b>Setting</b>	<b>Description</b>
	Select the Delete TAI button to delete this TAI from your test configuration.
<b>PLMN ID:</b> 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.
<b>TAC:</b>	
	Select the Add TAC button to add a new TAC (Tracking Area Code) to your test configuration.
<b>Settings:</b>	
	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.

### Cell ID List

The following table describes the configuration settings that are required for Cell ID.

<b>Setting</b>	<b>Description</b>
<b>Cell ID:</b>	
	Select the Add Cell ID button to add a new UE ID to your test configuration.
<b>Cell ID settings:</b>	
	Select the Delete Cell ID button to delete the UE ID from your test configuration.
<b>PLMN ID:</b> Set the values for the PLMN identifier.	
PLMN MCC	The PLMN Mobile Country Code (MCC) used in the construction of the Cell ID.
PLMN MNC	The PLMN Mobile Network Code (MNC) used in the construction of the Cell ID.
Cell ID	The cell identifier of the UE.

### MME Configuration Update

The following table describes the configuration settings that are required for MME Configuration Update.

Setting	Description
<i>MME Configuration Update(s):</i>	
	Select the Add MME Configuration Update(s) button to configure a new MME Configuration Update message.
<i>MME Configuration Update:</i>	
	Select the Delete MME Configuration Update button to delete the MME Configuration Update message configuration.
Delay (ms)	The delay between S1 setup and the first MME Configuration Update, or between subsequent MME Configuration Update procedures.
<i>Updated Item(s):</i>	
	Select the Add Updated Item button to add a new item to be updated.
<i>Updated Item:</i>	
	Select the Delete Updated Item button to delete this item from your test configuration.
Type	Select one of the update options: <ul style="list-style-type: none"> <li><b>Updated MME Name</b> - refers to the MME instance name (see <b>Value</b>)</li> <li><b>Updated Relative Capacity</b> - refers to the MME instance relative capacity (see <b>Value</b>)</li> <li><b>Supplementary GUMMEI</b> - the MME Configuration Update messages for Supplementary GUMMEI will always include the GUMMEI original values (at S1 setup), besides the ones in the update, to avoid impact on the current test.</li> </ul>
Value	If <b>Type</b> is set as: <ul style="list-style-type: none"> <li><b>Updated MME Name</b> - it will allow you to update the unique name that identifies the selected MME instance.</li> <li><b>Updated Relative Capacity</b> - will allow to update the relative capacity value, which should be between 0 and 255.</li> </ul>
MCC	<div style="border: 1px solid #ccc; padding: 2px;"><b>NOTE</b></div> This parameter appears when <b>Type</b> is set as <b>Supplementary GUMMEI</b> . The MCC for this MME range.
MNC	<div style="border: 1px solid #ccc; padding: 2px;"><b>NOTE</b></div> This parameter appears when <b>Type</b> is set as <b>Supplementary GUMMEI</b> . The MNC for this MME range.

Setting	Description
Group ID	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUMMEI</b>.</p> <p>Set the MME group ID value.</p>
Code	<p><b>NOTE</b> This parameter appears when <b>Type</b> is set as <b>Supplementary GUMMEI</b>.</p> <p>Set the MME code value.</p>

## 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.
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.

S1 Interface 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.
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

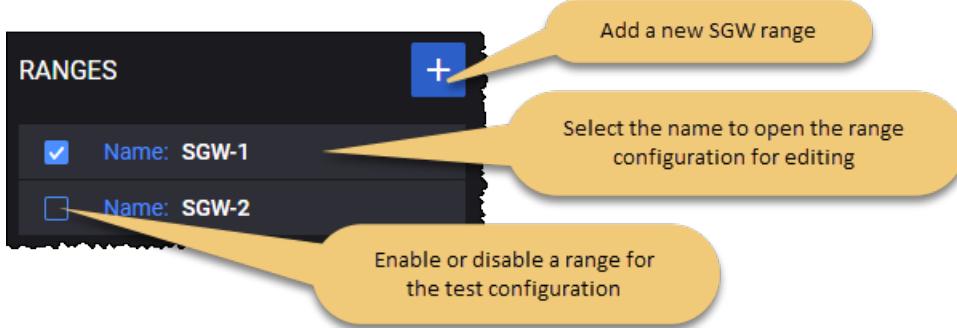
## SGW Ranges configuration settings

To access and configure the SGW ranges settings, select **SGW Ranges** from the Core Ranges panel.

You can perform the following tasks from the **SGW Ranges** panel:

- Add a new SGW range to your test configuration.
- Open a SGW range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



You add and select SGW ranges from the Ranges panel. When you select the name of a SGW, 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 <b>Delete Range</b> 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"> <li>• minimum: 212992 #The default Linux buffer size</li> <li>• maximum: 134217728 #128MB</li> <li>• default: 12582912 #12MB</li> </ul>
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> <li>• minimum: 212992 # The default Linux buffer size</li> <li>• maximum: 134217728 #128MB</li> <li>• default: 2097152 #2MB</li> </ul>
S1-u Interface Settings	These settings are described in <a href="#">SGW S1-u interface settings</a> .

## SGW S1-u interface settings

The following **Connectivity Settings** enable the necessary S1-u connectivity and service interaction.

S1-u Interface Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>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 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.
<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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN</i></p>

S1-u Interface Settings	Description
	<i>to open the configuration panel for editing.</i>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

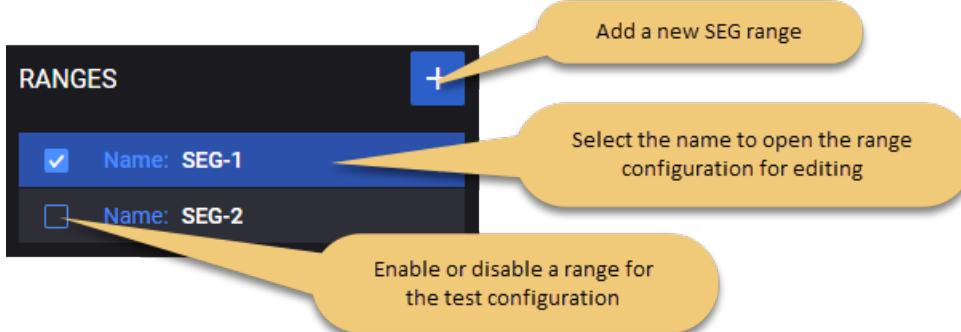
## SEG Ranges configuration settings

To access and configure the SEG ranges settings, select **SEG Ranges** from the CoreSim panel.

You can perform the following tasks from the **SEG Ranges** panel:

- Add a new SEG range to your test configuration.
- Open a SEG range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



You add and select SEG ranges from the SEG Ranges panel. When you select the name of a SEG , 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
Range:	

Setting	Description
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 <b>Delete Range</b> 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 <b>Responder (Remote Access)</b> and cannot be changed.
UDP Rx Buffer (bytes)	Size of receive buffers for UDP sockets: <ul style="list-style-type: none"> <li>minimum: 212992</li> <li>maximum: 134217728</li> <li>default: 12582912</li> </ul>
UDP Tx Buffer (bytes)	Size of transmit buffers for UDP sockets: <ul style="list-style-type: none"> <li>minimum: 212992</li> <li>maximum: 134217728</li> <li>default: 2097152</li> </ul>
<i>Interface Settings</i>	<i>These settings are described in <a href="#">SEG interface settings</a>.</i>
<i>Remote Access IP Pool</i>	
Start IP	Set the start IP address.
IP Increment	Set the IP address increment value.
IPs count	Set the IP count value.
IP Prefix Length	Set the IP prefix length value.
<i>Local Protected Subnet</i>	<i>Selects which node(s) are protected by SEG: AMF and/or UPF . AMF and UPF could be protected by the same SEG when running with Linux stack.</i>
N2 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific AMF range from the list.
N3 Host(s)	Select an entry from the drop-down list: you can either <i>Select All</i> or select a specific UPF range from the list.

<b>Setting</b>	<b>Description</b>
<i>Authentication</i>	
Authentication Method	By default, the authentication method is set to <b>Certificates</b> and cannot be changed.
CA Certificate	Select the <a href="#">CA certificate</a> 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 SEG range, using the <b>Upload</b> button. To remove the archive , select the <b>Clear</b> button.</p> <p>The <code>.key</code> and <code>.crt</code> files need to have the same name before extensions.</p>
<i>Use Same Certificates and Private Key For All Tunnels</i>	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: <b>AES-128-GCM-16</b>. Available options: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b>.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: <b>NONE</b>. Available options: <b>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</b>.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> <li>• When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>• If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
DH Group	<p>Select an option from the drop-down list.</p> <p>Default value: <b>prime256v1(19)</b>. Available options: <b>prime256v1(19), secp384r1(20), secp521r1(21), prime192v1(25), secp224r1(26), x25519(31), x448(32)</b>.</p>
PRF Algorithm	<p>Select an option from the drop-down list.</p> <p>Default value: <b>HMAC-SHA256</b>. Available options: <b>HMAC-MD5, HMAC-SHA1, HMAC-SHA256, HMAC-SHA384, HMAC-SHA512</b>.</p>
<i>IKE Phase 2</i>	

<b>Setting</b>	<b>Description</b>
Encryption Algorithm	<p>Select the encryption algorithm from the drop-down list.</p> <p>Default value: <b>AES-128-GCM-16</b>. Available options: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b>.</p>
Hash Algorithm	<p>Select the hash algorithm from the drop-down list.</p> <p>Default value: <b>NONE</b>. Available options: <b>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</b>.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> <li>• When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>• If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
<i>Identification</i>	
Local Identification Type	<p>Select an option from the drop-down list.</p> <p>Default value: <b>ID_DER ASN1 DN</b>. Available options: <b>ID_IPV4_ADDR, ID_FQDN, ID_USER_FQDN, ID_IPV6_ADDR, ID_DER ASN1 DN, ID_KEY_ID</b>.</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: <b>ID_FQDN, ID_KEY_ID or ID_RFC822_ADDR</b>.</p>
<i>Timers</i>	
Enable Rekey	<p>By default, this option is disabled. Select the toggle button to enable it.</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>
IKE Phase 1 (IKE) Lifetime (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>
DPD Interval (s)	<p>Set a value for this parameter.</p> <p>Default value: <b>0</b> (disabled).</p>

## SEG interface settings

The following **Connectivity Settings** enable connectivity and service interaction.

SEG Interface Settings	Description
Source Port	Set the source port number.
Enable NAT-T	Select to enable the NAT Traversal keepalive.
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i> ). The default value is 000000000001.
<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.
Inner VLAN	<p><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

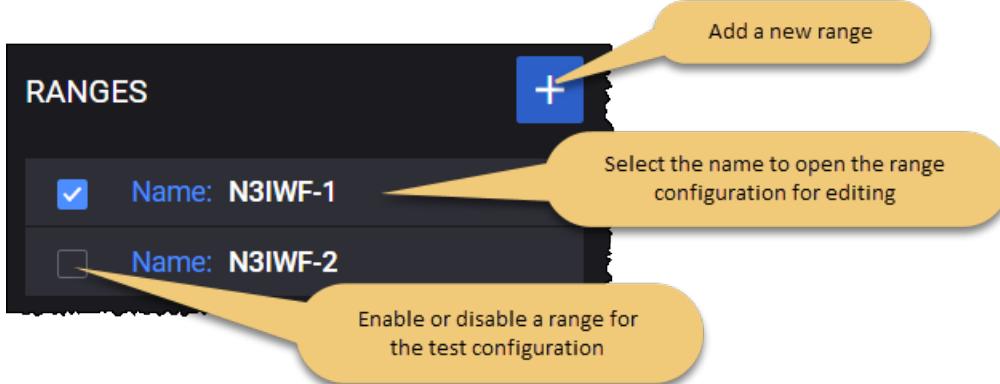
## N3IWF Ranges configuration settings

To access and configure the N3IWF ranges settings, select **N3IWF Ranges** from the CoreSim panel.

You can perform the following tasks from the **N3IWF Ranges** panel:

- Add a new N3IWF range to your test configuration.
- Open a N3IWF range configuration (for editing or viewing).
- Enable or disable a range for the test configuration.

**For example ...**



You add and select N3IWF ranges from the N3IWF Ranges panel. When you select the name of a N3IWF, LoadCore opens the **Range** panel, from which you can:

- Delete the N3IWF range from the test configuration.
- Designate the range as a **Device Under Test**.
- Modify the N3IWF range name.
- Configure the range and connectivity settings for the N3IWF range.

### N3IWF range controls and settings

Each N3IWF range is identified by a unique name. You can add and delete N3IWF ranges as necessary to support your test objectives.

The following table describes the **Range Settings** that you configure for each N3IWF range.

Setting	Description
<i>Range:</i>	
Device Under Test	Enable this option if your N3IWF is a DUT in this test configuration. When this option is not enabled, the LoadCore will simulate the N3IWF functionality (if it is selected in the Topology window).
	Select the <b>Delete Range</b> button to delete this range from your test configuration.
<i>Range Settings:</i>	
<i>Node Settings</i>	
Name	The name uniquely identifies each N3IWF instance. You can accept the value

<b>Setting</b>	<b>Description</b>
	provided by LoadCore or overwrite it with your own value.
Role	By default, the role is set to <b>Responder (Remote Access)</b> and cannot be changed.
PLMN MCC	<p>The PLMN MCC for this N3IWF range.</p> <p><b>About PLMN MCC ...</b></p> <p>A Public Land Mobile Network (PLMN) is a telecommunications network that provides wireless communication services offered by a specific operator in a specific country. A PLMN is identified by a globally unique PLMN code, which consists of a MCC (Mobile Country Code) and MNC (Mobile Network Code). It is a five- to six-digit number identifying a country, and a mobile network operator in that country, usually represented in the form 001-01 or 001-001.</p> <p>The Mobile Country Code (MCC) is a three-digit code that uniquely identifies the country of domicile of the mobile subscriber.</p>
PLMN MNC	<p>The PLMN MNC for this N3IWF range.</p> <p><b>About PLMN MNC ...</b></p> <p>The Mobile Network Code (MNC) is a two-digit (North America) or three-digit (European Standard) code that is used in combination with a Mobile Country Code (MCC) to uniquely identify a mobile network operator. The MCC-MNC tuple is stored within the first five or six digits of the IMSI (International Mobile Subscriber Identity), and is also used in combination with the MCC to identify a PLMN.</p>
Tracking Area Code	Provide the Tracking Area Code (TAC) value
N3IWF ID	Set the value for this field.
N3IWF ID Increment	Set the increment value for this field.
SCTP Tx Buffer (bytes)	Set the size of SCTP Tx Buffer.
SCTP Rx Buffer (bytes)	Set the size of SCTP Rx Buffer.
UDP Rx Buffer (bytes)	<p>Size of receive buffers for UDP sockets:</p> <ul style="list-style-type: none"> <li>• minimum: 212992</li> <li>• maximum: 134217728</li> <li>• default: 12582912</li> </ul>
UDP Tx Buffer (bytes)	<p>Size of transmit buffers for UDP sockets:</p> <ul style="list-style-type: none"> <li>• minimum: 212992</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>maximum: 134217728</li> <li>default: 2097152</li> </ul>
Traffic Profiles	These settings are described in <a href="#">Traffic Profiles settings</a> .
NSSAI	These settings are described in <a href="#">NSSAI settings</a> .
NWu Interface Settings	These settings are described in <a href="#">N3IWF interface settings</a> .
N2 Interface Settings	These settings are described in <a href="#">N3IWF interface settings</a> .
N3 Interface Settings	These settings are described in <a href="#">N3IWF interface settings</a> .
Authentication	
Configure Certificates	By default, this option is disabled. When enabled, the following fields become available: <i>Certificates(.zip)</i> and <i>Use Same Certificate For All Instances</i> .
CA Certificate	Select the CA Certificate from the drop-down list.  NOTE To be able to populate and select from the drop-down, you first need to upload certificates.
Certificates (.zip)	It allows you to upload an archive that contains the certificates for the N3IWF range, using the <b>Upload</b> button. To remove the archive , select the <b>Clear</b> button.
Use Same Certificates For All Instances	By default, this option is disabled. Select the toggle button to enable it.
IKE Phase 1	
Encryption Algorithm	Select the encryption algorithm from the drop-down list.  Default value: <b>AES-128-GCM-16</b> . Available options: <b>AES-128-CBC, AES-192-CBC, AES-256-CBC, AES-128-GCM-16, AES-192-GCM-16, AES-256-GCM-16</b> .
Hash Algorithm	Select the hash algorithm from the drop-down list.  Default value: <b>NONE</b> . Available options: <b>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</b> .  Restrictions: <ul style="list-style-type: none"> <li>When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16, AES-192-GCM-16 or AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> </ul>

Setting	Description
	<ul style="list-style-type: none"> <li>If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
DH Group	Select an option from the drop-down list. Available options are: <b>modp768(1)</b> , <b>modp1024(2)</b> , <b>modp1536(5)</b> , <b>modp2048(14)</b> , <b>modp3072(15)</b> , <b>modp4096(16)</b> , <b>modp6144(17)</b> , <b>modp8192(18)</b> , <b>prime256v1(19)</b> , <b>secp384r1(20)</b> , <b>secp521r1(21)</b> , <b>prime192v1(25)</b> , <b>secp224r1(26)</b> , <b>x25519(31)</b> , <b>x448(32)</b> . Default value: <b>prime256v1(19)</b> .
PRF Algorithm	Select an option from the drop-down list. Default value: <b>HMAC-SHA256</b> . Available options: <b>HMAC-MD5</b> , <b>HMAC-SHA1</b> , <b>HMAC-SHA256</b> , <b>HMAC-SHA384</b> , <b>HMAC-SHA512</b> .
<i>IKE Phase 2</i>	
Encryption Algorithm	Select the encryption algorithm from the drop-down list. Default value: <b>AES-128-GCM-16</b> . Available options: <b>AES-128-CBC</b> , <b>AES-192-CBC</b> , <b>AES-256-CBC</b> , <b>AES-128-GCM-16</b> , <b>AES-192-GCM-16</b> , <b>AES-256-GCM-16</b> .
Hash Algorithm	Select the hash algorithm from the drop-down list. Default value: <b>NONE</b> . Available options: <b>NONE</b> , <b>HMAC-MD5-96</b> , <b>HMAC-SHA1-96</b> , <b>HMAC-MD5-128</b> , <b>HMAC-SHA1-160</b> , <b>HMAC-SHA2-256-128</b> , <b>HMAC-SHA2-384-192</b> , <b>HMAC-SHA2-512-256</b> . Restrictions: <ul style="list-style-type: none"> <li>When <i>Encryption Algorithm</i> is set to one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the only available <i>Hash Algorithm</i> is <b>NONE</b>.</li> <li>If <b>Encryption Algorithm</b> is set to a value other than one of <b>AES-128-GCM-16</b>, <b>AES-192-GCM-16</b> or <b>AES-256-GCM-16</b>, the <b>NONE</b> hash algorithm is not available.</li> </ul>
<i>Identification</i>	
Local Identification Type	Select an option from the drop-down list. Default value: <b>ID_DER ASN1 DN</b> . Available options: <b>ID_IPV4_ADDR</b> , <b>ID_FQDN</b> , <b>ID_USER_FQDN</b> , <b>ID_IPV6_ADDR</b> , <b>ID_DER ASN1 DN</b> , <b>ID_KEY_ID</b> .
Local Identification Value	Set the value for this parameter. This field is mandatory if the <i>Local Identification Type</i> is set to: <b>ID_FQDN</b> , <b>ID_KEY_ID</b> or <b>ID_RFC822_ADDR</b> .

Setting	Description
Timers	
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: <b>0</b> (disabled).
IKE Phase 1 (IKE) Lifetime (s)	Set a value for this parameter. Default value: <b>0</b> (disabled).
DPD Interval (s)	Set a value for this parameter. Default value: <b>0</b> (disabled).

### Traffic Profiles

The following table describes the configuration settings that are required for Control Plane.

**NOTE** Only one Control Plane Profile is accepted.

Setting	Description
TCP Port	The TCP port for N3IWF: <ul style="list-style-type: none"><li>• default value: <b>20000</b>.</li><li>• minimum value: <b>1024</b>.</li><li>• maximum value: <b>65535</b>.</li></ul>
IP Type	Select the IP type from the drop-down list: <b>IPv4</b> (default) or <b>IPv6</b> .
Local Protected Subnet IP Address	The IP address for N3IWF TCP server. Default value: <b>150.0.2.1</b> .
Local Protected Subnet IP Prefix Length	The only accepted options are <b>32</b> for IPv4 and <b>128</b> for IPv6.
Remote Inner IP Address	Per UE IP Address used for TCP Control Plane connection. Address increment is 1. Default value: <b>150.0.100.1</b> .

The following table describes the configuration settings that are required for User Plane.

**NOTE** A maximum of 15 User Plane Profile can be configured.

Setting	Description
	Select the Add User Plane button to add a new profile to your test configuration.
	Select the Delete User Plane button to delete this profile from your test configuration.
DNN	Select the DNN value for the drop-down list.
IP Type	Select the IP type from the drop-down list: <b>IPv4</b> (default) or <b>IPv6</b> .
Local Protected Subnet IP Address	The IP address for N3IWF GRE endpoint. Default value: <b>150.1.2.1</b> .
Local Protected Subnet IP Prefix Length	The only accepted options are <b>32</b> for IPv4 and <b>128</b> for IPv6.
Remote Inner IP Address	Per PDU Session IP Address used for GRE User Plane connection. Address increment is 1. Default value: <b>150.1.100.1</b> .

## NSSAI

The following table describes the configuration settings that are required for NSSAI.

Setting	Description												
<b>NSSAI:</b>													
	Select the Add NSSAI button to add a new NSSAI to your test configuration.												
<b>NSSAI settings:</b>													
	Select the Delete NSSAI button to delete this NSSAI from your test configuration.												
SST	The value that identifies the SST (Slice/Service Type) for this NSSAI. SST comprises octet 3 in the NSSAI information element. The standardized SST values are: <table border="1" data-bbox="344 1543 1437 1776"> <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												

Setting	Description
	field comprises octets 4 through 6 in the NSSAI.

## N3IWF interface settings

### NWu interface settings

The following settings enable connectivity and service interaction.

Interface Settings	Description
Source Port	Set the source port number.
Enable NAT-T	Select to enable the NAT Traversal keepalive.

Connectivity Settings	Description
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i> ). The default value is 000000000001.

<b>Connectivity Settings</b>	<b>Description</b>
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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN 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.

## N2 interface settings

The following settings enable connectivity and service interaction.

<b>Interface Settings</b>	<b>Description</b>
Peer AMF	The IP address of the AMF node connected over the N2 interface.
Destination port	The destination Stream Control Transmission Protocol (SCTP) port for control plane messages (NG-AP signaling messages) on the N2 interface.
SCTP source port	The source SCTP port for control plane messages (NG-AP signaling messages). Each SCTP endpoint provides the other endpoint with a list of transport addresses through which that endpoint can be reached and from which it will originate SCTP packets. These transport addresses are composed of multiple IP addresses in combination with an SCTP port. The default port number is 36412, but you can change it.
Connection Timeout (ms)	Set the connection timeout value.
<i>SCTP Parameters</i>	
Avoid Bundling of Data Chunks	Select this option to enable it. It turns on/off any Nagle-like algorithm. This means that packets are generally sent as soon as possible and no unnecessary delays are introduced, at the cost of more packets in the network.
Minimum Retransmission Timeout (ms)	Set the minimum retransmission timeout value, in milliseconds.
Maximum	Set the maximum retransmission timeout value, in milliseconds.

<b>Interface Settings</b>	<b>Description</b>
Retransmission Timeout (ms)	
Initial Retransmission Timeout (ms)	Set the initial retransmission timeout value, in milliseconds.
Maximum Retransmission per Association	Set the maximum retransmissions value per association.
Maximum Retransmission per Path	Set the maximum retransmissions value per path.
Heartbeat Interval (ms)	Set the heartbeat interval value, in milliseconds.
SACK Delay (ms)	Set the delayed selective ACK timeout value.
SACK Frequency	Set the delayed selective ACK frequency value.
<b>Connectivity Settings</b>	<b>Description</b>
IP	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
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.

<b>Connectivity Settings</b>	<b>Description</b>
MSS	The Maximum Segment Size (MSS) for this range. MSS specifies the largest TCP segment that the IP device can transmit as a single, unfragmented unit.
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
MAC	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i> ). The default value is 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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

## N3 interface settings

The following **Connectivity Settings** enable connectivity and service interaction.

<b>SEG Interface Settings</b>	<b>Description</b>
<i>IP</i>	<i>Select the IP address to open the IP configuration panel for editing.</i>
IP Address	The IP address in your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
Gateway Address	The IP address assigned as gateway address.
Gateway Increment	The value to use when incrementing the Gateway address (starting with the Gateway Address).
<i>Additional Routes</i>	<i>The additional routes will use the gateway defined in the IP information below.</i>
	Select this button to add a new additional route to your test configuration, if needed.
	Select this button to remove the additional route to your test configuration.
IP Address	The IP address from your test network to use for traffic on this interface.
IP Prefix Length	The IP address prefix assigned to this range. It specifies the number of leftmost bits in the address, which indicates the network portion of the address.
<i>MAC</i>	<i>Select the MAC address to open the MAC configuration panel for editing.</i>
MAC Address	Hardware MAC address.
MAC Increment	The value to use when incrementing the MAC address (starting with the <i>MAC Address</i> ). The default value is 000000000001.
<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><b>IMPORTANT</b> <i>This option is visible only when the Outer VLAN is selected.</i></p> <p><i>Select the check-box to make this option available, and then select the Inner VLAN to open the configuration panel for editing.</i></p>

<b>SEG Interface Settings</b>	<b>Description</b>
VLAN ID	VLAN identifier.
VLAN TPID	VLAN tag protocol ID.

**CHAPTER 12**

## Manage LoadCore licenses

---

LoadCore is a licensed product. You can manage licenses using either the integrated LoadCore License Manager or a centralized License server that is managed by your organization.

**Chapter contents:**

<b>Licensing Requirements</b> .....	<b>1239</b>
<b>License Manager</b> .....	<b>1239</b>
<b>License Server</b> .....	<b>1241</b>
<b>Licensed Test Configs</b> .....	<b>1242</b>

## 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.

## License Manager

The first time you use LoadCore, you need to active at least one license. You activate and manage your licenses using the LoadCore **License Manager** functions, which are accessed from the setup menu.

- [How to open License Manager on the next page](#)
- [Activate a license on the next page](#)
- [Deactivate a license on the next page](#)
- [Sync licenses on the next page](#)
- [Reserve a license on the next page](#)
- [Get license statistics on page 1241](#)
- [Perform offline license operations on page 1241](#)

## How to open License Manager

To access the LoadCore License Manager:

1. Select **Administration** from the setup menu (⚙).
2. Select **License Manager** (from the **Administration** menu).

## Activate a license

To activate one or more LoadCore licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **Activate licenses**.  
LoadCore opens the **Activate Licenses** dialog.
3. Enter your license data in the dialog box.  
You can use either activation codes or entitlement codes (one or more ).
4. Select **Load Data**, indicate the number of licenses you want to activate, then click **Activate**.

Your new licenses—which should now be listed in the License Manager page—are now available for running tests.

## Deactivate a license

To deactivate one or more LoadCore licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **Deactivate licenses**, then and indicate a new quantity for each of the existing licenses.
3. Select **Perform the Activation** to complete the task.

**NOTE** It is recommended to deactivate the license before deleting a LoadCore VM. This way you can easily reuse the same license (Activation Code) when deploying another LoadCore VM.

## Sync licenses

To synchronize one or more LoadCore licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **Sync licenses**.

## Reserve a license

To reserve one or more LoadCore licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select the **Manage Reservation** icon.  
LoadCore opens a new window.
3. Select the license you wish to reserve.
4. Enter the number of desired licenses in **New Reserved Count** field.
5. Enter the duration of the reservation (in hours) in the **Duration to Reserve** field.

**NOTE**

The License Statistics display shows all reserved features, ordered by count and reserved time. The initial reserved count and duration is overwritten when a new reservation is performed.

## Get license statistics

To activate one or more LoadCore licenses:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **License statistics**.

## Perform offline license operations

Offline license management is required for cases in which your test network is operating in an isolated environment with no Internet access. To perform offline LoadCore license operations:

1. Select **Administration** from the setup menu (⚙), then select **License Manager**.
2. Select **Offline operations**.  
LoadCore opens the **Keysight Licensing Offline Operations** dialog.
3. Click **Generate request**.
4. Using a system that has Internet connectivity, access the KSM Offline Operations Page, and follow the steps provided for the desired operation.
5. From your offline system, return to the **Keysight Licensing Offline Operations** dialog, then click **Import license**.
6. Click **Finish** to complete the task.

## License Server

Rather than using the internal LoadCore License Manager, you can use a centralized License server that is managed by your organization.

### Add a License Server

To add a license server in the LoadCore web UI:

1. Log in the LoadCore web UI.
2. Under the Settings Menu (⚙), select License Servers.

The dialog shows the license server currently used.

**NOTE**

To see the list of installed licenses, you need to access the license server in a web browser: <https://<license-Server-IP>>

3. Enter the license server IP address in the empty license server field, then select the Add button (+) next to the field.
4. Select **CLOSE** to confirm your action and close the License server dialog.

### Remove a License Server

To remove a license server that was previously added in the LoadCore web UI:

1. Log in the LoadCore web UI.
2. Under the Settings menu (⚙), select License servers.  
The license servers dialog opens, listing the previously-set license servers.
3. Select the **Delete** button next to the license server that you want to remove.
4. Select **CLOSE** to confirm your action and close the License server dialog.

## Activate a license

To activate one or more LoadCore licenses:

1. From the Setting menu (⚙), select **Application Settings**.  
LoadCore opens the **Applications Settings** dialog.
2. Select a **License Provider** from the drop-down list.
3. Enter the IP address in the **License Server IP** field.
4. Click **Update**.

## 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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 Dereistration 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 101.2 Single	<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>

<b>Test Case</b>	<b>Test Case Description</b>
UE Force Emergency Registration No PDU Session SUCI Null	<p>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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 101.4 AMF triggers identification procedure to get UE identity during Registration	<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 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 101.5 UE registers perodic 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 102 Single UE Reg 1 PDU 1 Flow SUCI Null De-Reg	<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>

<b>Test Case</b>	<b>Test Case Description</b>
UDP	<p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 106 Single UE Reg 1 PDU 2 Flows Same DNN (1x TCP 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>

<b>Test Case</b>	<b>Test Case Description</b>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 108.3 Single UE with UDP HTTP and Voice traffic	<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 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> </ul>

<b>Test Case</b>	<b>Test Case Description</b>
	<ul style="list-style-type: none"> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation	This test verifies that 10 UEs can register in to the 5G Core Network at a rate

<b>Test Case</b>	<b>Test Case Description</b>
TC 117 10 UEs Reg Rate 1/s 1 PDU 1 Flow De-Reg	<p>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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation	This test verifies that 5G Core Network can support 48 gNBs with 1000 UEs,

<b>Test Case</b>	<b>Test Case Description</b>
TC 703 1000UEs and 90GB-HTTP Get Traffic with FourPort Pairs	<p>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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
gNB Simulation TC 705 5000UEs and 50GB- Data 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>, 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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>

<b>Test Case</b>	<b>Test Case Description</b>
	<ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
AMF Isolation TC 106 Single UE Reg 1 PDU 2 Flows Same DNN (1x TCP 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
AMF Isolation TC 110 Single UE	<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</p>

<b>Test Case</b>	<b>Test Case Description</b>
Reg 1 PDU 1 Flow Multiple HO De-Reg UDP	<p>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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
AMF Isolation 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> </ul>

<b>Test Case</b>	<b>Test Case Description</b>
	<ul style="list-style-type: none"> <li>• <b>B2B</b> - DUT not deployed</li> </ul> <p>AMF Isolation TC 116 10 UEs Reg 1 PDU 1 Flow Multiple HO and Enter/Exit Idle Rate 1/s De-Reg UDP</p> <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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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	<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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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>

Test Case	Test Case Description
	<ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>

## 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
UDM Isolation TC 102 Registration and Deregistration AMF to UDM	<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> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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</p>

Test Case	Test Case Description
	<p>5.1.1.</p> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> </ul>

<b>Test Case</b>	<b>Test Case Description</b>
	<ul style="list-style-type: none"> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
PCF Isolation TC 132 SM Policy Association Modification Trigger PLMN_CH (PLMN Change)	<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> <ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
PCF Isolation TC 136 SM Policy Association Modification	<p>This test verifies that the SMF can initiate an Update policy using the trigger when the PDU Session or the Monitoring key specific</p>

<b>Test Case</b>	<b>Test Case Description</b>
Trigger US_RE (PDU Threshold)	<p>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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> </ul>

<b>Test Case</b>	<b>Test Case Description</b>
	<ul style="list-style-type: none"> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
PCF Isolation TC 145 SM Policy Association Modification Trigger NO_CREDIT (Out of Credit)	<p>This test verifies that the SMF can initiate an Update policy using 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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>

<b>Test Case</b>	<b>Test Case Description</b>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
PCF Isolation TC 151 SM Policy Association Modification Trigger SUCC_RES_ALLO (Success Rule Release)	<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> <p>This test case is available in two scenarios:</p> <ul style="list-style-type: none"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>
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"> <li>• <b>Live</b> - DUT deployed</li> <li>• <b>B2B</b> - DUT not deployed</li> </ul>

## Licensed UPF Isolation Configs

The following test cases are available in the current release of LoadCore.

<b>Test Case</b>	<b>Test Case Description</b>
TC-01 UPF Isolation 1000 UE 400Kbps Per UE 400Mbps HTTP	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.

<b>Test Case</b>	<b>Test Case Description</b>
Throughput	
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 UE 20Gbps HTTP Throughput	This test validates real UPF performance when 50K UEs are generating 20Gbps HTTP Throughput in the DL. UE DL AMBR 400Kbps & UL 10Kbps, 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 10Kbps, 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 200Kbps, 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.

<b>Test Case</b>	<b>Test Case Description</b>
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 200Kbps, 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 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.
TC-14 UPF Isolation 600K UE 100 Kbps Per UE 60Gbps HTTP Throughput	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.
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 10Kbps, QFI 5, 6, 7 used in the test to send 6PDRs.

This page intentionally left blank.

**CHAPTER 13**

## Manage LoadCore users

---

Managing the users who can access the application is one of the primary LoadCore administrative requirements.

- [User categories below](#)
- [Creating users below](#)
- [Reset a user's password on the next page](#)
- [Disable a user account on the next page](#)
- [Delete a user account on the next page](#)

### User categories

LoadCore user accounts can be of one of the following types:

- Administrative user: Can access the Access Control functions and perform various administrative tasks, including the definition and management of other user accounts.
- Regular user: Can access the application and use all of the resources involved in test creation, execution, and analysis.

### Creating users

Each user who requires access to the LoadCore application must have a user account. To add a user:

1. Select the settings menu ( ) and then select **Administration**.
2. Select **Access Control** from the **Administration** menu.  
LoadCore opens the **Keycloak Admin Console** in a new browser tab.
3. Select **Users** from the list of **Manage** functions (in the navigation pane).
4. Select the **Add user** button.
5. Enter the required information in the **Add user** form, then select the **Save** button.  
The following values are required for the new user:
  - Username (which must be unique within the realm).
  - Email address
  - First and Last Name
  - *User Enabled* set to **ON**.
6. Select the **Save** button.  
LoadCore adds the user and displays that user's information in the **Details** tab.
7. Set the initial password for the user:
  - a. Select the **Credentials** tab.
  - b. Enter the *Password*.
  - c. Re-enter the password in the *Password Confirmation* field.
  - d. Set **TemporaryON** if the user will be required to change the password upon initial log in.
  - e. Select the **Set Password** button.

LoadCore displays a confirmation dialog.

- f. Select the **Set Password** button to confirm the action.

## Reset a user's password

Administrative users can reset a user's password:

1. Select the settings menu (⚙) and then select **Administration**.
2. Select **Access Control** from the **Administration** menu.  
LoadCore opens the **Realm Settings** window.
3. Select **Users** from the list of **Manage** functions.
4. Select the user.
5. Select the **Credentials** tab.
6. Enter the new *Password*.
7. Re-enter the new password in the *Password Confirmation* field.
8. Set *Temporary* **ON** if the user will be required to change the password upon initial log in.
9. Select the **Reset Password** button.  
LoadCore displays a confirmation dialog.
10. Select the **Reset Password** button to confirm the action.

## Disable a user account

Administrative users can temporarily disable a user's account:

1. Select the settings menu (⚙) and then select **Administration**.
2. Select **Access Control** from the **Administration** menu.  
LoadCore opens the **Realm Settings** window.
3. Select **Users** from the list of **Manage** functions.
4. Select the user.
5. Set *User Enabled* to **OFF**.

This user account will not be able to log in until the account access is set to **ON**.

## Delete a user account

Administrative users can reset a user's password:

1. Select the settings menu (⚙) and then select **Administration**.
2. Select **Access Control** from the **Administration** menu.  
LoadCore opens the **Realm Settings** window.
3. Select **Users** from the list of **Manage** functions.
4. View all users or search for the Username of the account that you will delete.
5. Click **Delete**.

The screenshot shows a user management interface. At the top, there is a search bar with the text 'helene'. To the right of the search bar are buttons for 'View all users', 'Unlock users', and 'Add user'. Below the search bar is a table header with columns: ID, Username, Email, Last Name, First Name, and Actions. A single row of data is shown below the header, corresponding to the user 'helene'. The 'Actions' column for this user contains two buttons: 'Edit' and 'Delete'. The 'Delete' button is circled in red with a hand cursor icon pointing at it.

6. LoadCore opens a confirmation dialog.
7. Select **Delete** to confirm that you are permanently deleting this user account.

## Reset Password for Regular Users

This section describes the steps needed in order to reset the LoadCore log in password for regular users.

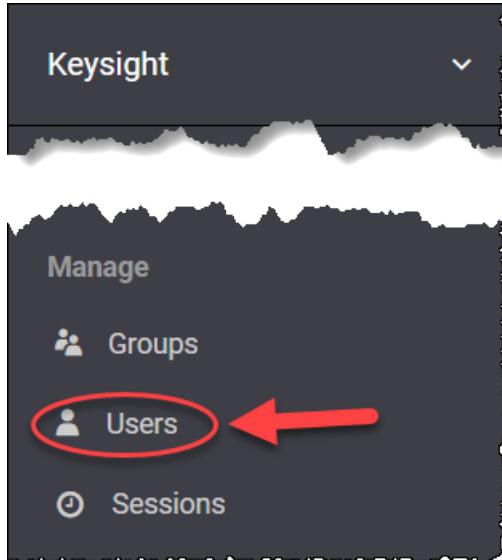
**IMPORTANT** The password can be changed only by an **ADMIN** user.

1. Select the wheel icon > **Administration**.

The screenshot shows a dark-themed administration menu. At the top right, there are icons for help, notifications, settings, and a user profile labeled 'admin'. Below these are several menu items: 'License Manager', 'Agent Management', 'Software Updates', 'Application Settings', and 'Administration'. The 'Administration' item is highlighted with a red circle and a hand cursor icon pointing at it.

A separate browser page opens, displaying all access control settings.

2. From the Manage section, select **Users**.



The Users section is displayed.

- From the Lookup tab, use the search function to find a specific user or select **View all users** to display all users and, then, select it from the list.

ID	Username	Email	Last Name	First Name	Actions
2527e098-9acd-48a9-8ab...	admin	admin@example.org	Admin	Default	<a href="#">Edit</a> <a href="#">Delete</a>
1a0287b9-9345-4858-b7b...	tester				<a href="#">Edit</a> <a href="#">Delete</a>

Select the **Edit** action for the user that needs a password reset. The user's profile section is displayed.

- Select **Credentials**.

Tester

Details	Attributes	Credentials	Role Mappings	Groups	Consents	Sessions
ID	1a0287b9-9345-4858-b7b6-f49d245a3a61					
Created At	4/18/22 12:59:58 PM					
Username	tester					

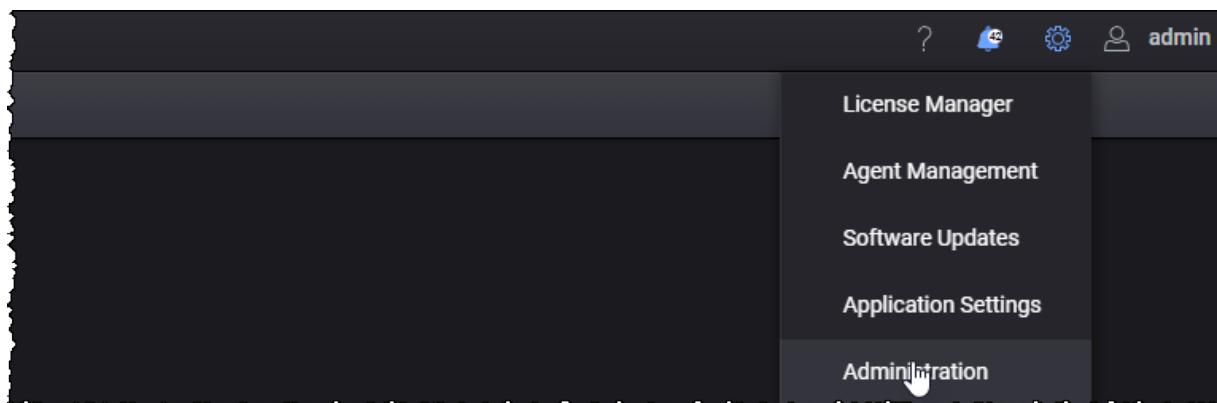
- Set the new password and select **Set Password** in order to apply the changes.

The screenshot shows the 'Manage Credentials' section for the 'Tester' user. It includes fields for 'Password' and 'Password Confirmation', both currently set to '.....'. A 'Temporary' toggle switch is set to 'ON'. The 'Set Password' button at the bottom is circled in red.

## 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:

The screenshot shows the 'User Federation > Add user storage provider' screen. The 'Enabled' switch is set to 'ON'. The 'Console Display Name' is 'ldap'. The 'Priority' is '0'. The 'Import Users' switch is set to 'ON'. The 'Edit Mode' dropdown is empty. The 'Sync Registrations' switch is set to 'OFF'. The 'Vendor' dropdown is set to 'Active Directory'. The 'Username LDAP attribute' is 'cn'. The 'RDN LDAP attribute' is 'cn'. The 'UUID LDAP attribute' is 'objectGUID'. The 'User Object Classes' is 'person, organizationalPerson, user'. The 'Connection URL' is 'ldap://keysight.com:389'. The 'Users DN' is 'cn=users,dc=ad,dc=keysight,dc=com'. The 'Custom User LDAP Filter' is '(objectclass=user)(objectcategory=person)(&(UserAccountControl:1.2.840.113556.1.4.803=-2))'. The 'Search Scope' is 'One Level'. The 'Bind Type' is 'simple'. The 'Bind DN' is 'cn=kcs\_system\_account,cn=users,dc=ad,dc=keysight,dc=com'. The 'Bind Credential' field contains a masked password. There are two blue buttons at the bottom right: 'Test connection' and 'Test authentication'.

- **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	!

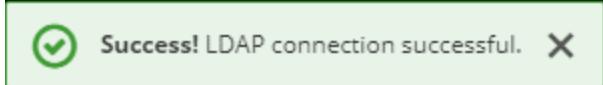
For Example:

```
(&(objectclass=user) (objectcategory=person) (!  
(UserAccountControl:1.2.840.113556.1.4.803:=2))) means "User AND Person AND  
Not Account Disabled"
```

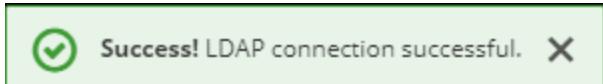
It reduced Users number from 26185 to 21262 in Keysight Active Directory on  
10/12/2020.

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.



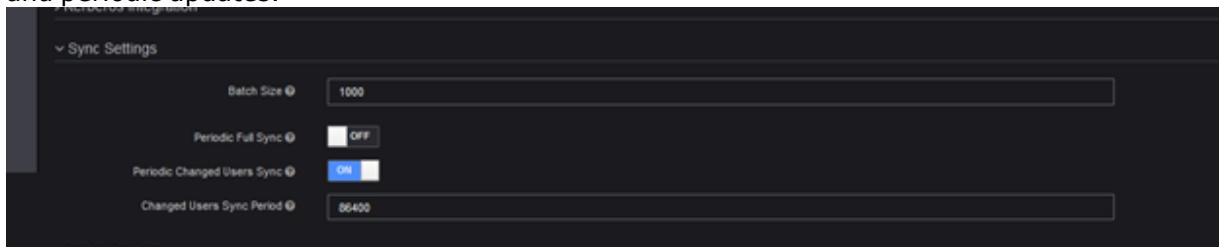
- **Test Authentication** - This button allows you to test if connection is correctly authenticated. After selecting the **Test Authentication** button success is indicated by a success message on the top of the page.



**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.



Success! Sync of users finished successfully. 0 imported users, 3355 updated users



**IMPORTANT**

It takes a long time to do a full synchronization. Wait until the success or failed message is displayed.

This page intentionally left blank.

*CHAPTER 14*

## 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:**

<b>Overview of passthrough testing .....</b>	<b>1272</b>
<b>Passthrough test configuration notes .....</b>	<b>1273</b>

# 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
- IPsec NG-RAN

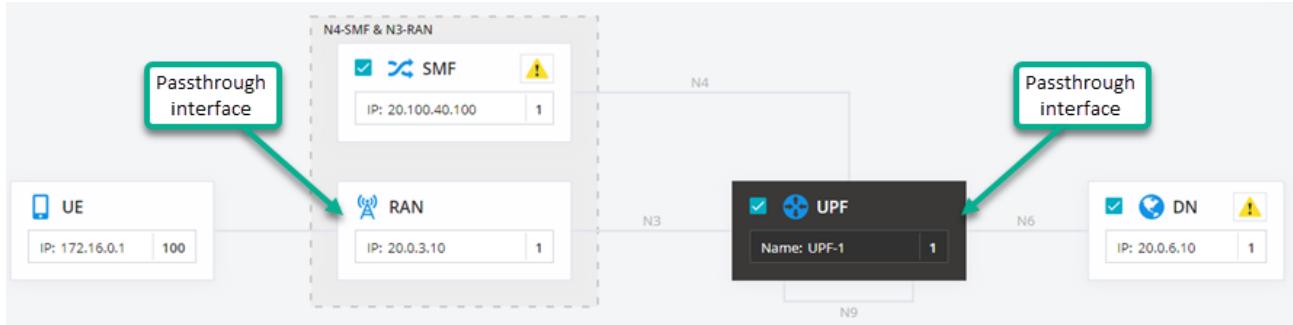
## Functional overview

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.
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.

 <b>RAN</b>	<ul style="list-style-type: none"> <li>• From the RAN <b>Range Settings</b>, select <b>Passthrough Interface Settings</b>, then select the <b>Connectivity Settings</b>. The <i>IP Address</i> that you configure will be the IP gateway address for the traffic sent from the external traffic source.</li> <li>• From the topology window, select the agent icon to open the <b>RAN Agent Assignment</b> window. In the <b>Passthrough Device</b> column, select a device that is not used by another interface in that test. This is the device from which the traffic is sent.</li> </ul>
--	---

### UE settings

The UE settings are the same for each of the test types that support passthrough testing.

 <b>UE</b>	<ul style="list-style-type: none"> <li>• From the UE <b>Range Settings</b>, select <b>Settings</b>, then select the <i>Enable Passthrough</i> option.</li> <li>• 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.</li> </ul>
---	--

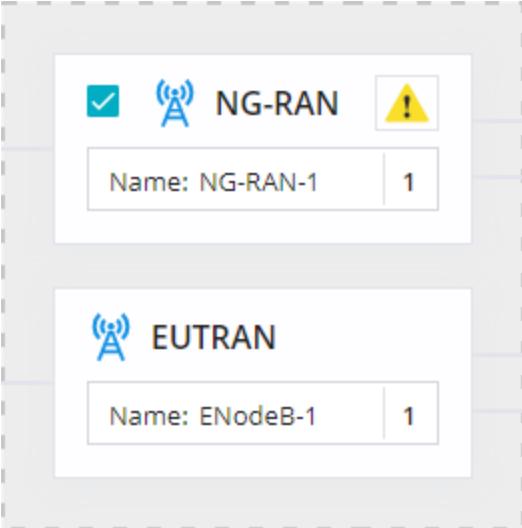
## UPF settings

The UPF settings are the same for each of the test types that support passthrough testing.

 UPF	<ul style="list-style-type: none"> <li>From the UPF <b>Range Settings</b>, select <b>N6 Interface Settings</b>, then select the <b>Connectivity Settings</b>. The <i>IP Address</i> that you configure will be the IP gateway address for the external server.</li> <li>From the topology window, select the agent icon to open the <b>UPF Agent Assignment</b> window. In the <b>N6</b> 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.</li> </ul>
---	---

## N4-SMF & N3-RAN settings

The UPF Isolation test type supports configuration of a passthrough interface, as follows:

	<ul style="list-style-type: none"> <li>From the RAN <b>Range Settings</b>, select <b>Passthrough Interface Settings</b>, then select the <b>Connectivity Settings</b>. The <i>IP Address</i> that you configure will be the IP gateway address for the traffic sent from the external traffic source.</li> <li>From the topology window, select the agent icon to open the <b>Agent Assignment</b> window. In the <b>Passthrough Device</b> column, select a device for this interface.</li> </ul>
--	--

## 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](#)

## APPENDIX A

# 5G abbreviations

---

The following list of abbreviations is based on the 3GPP technical specifications.

<b>Abbreviation</b>	<b>Description</b>
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

<b>Abbreviation</b>	<b>Description</b>
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)

<b>Abbreviation</b>	<b>Description</b>
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

<b>Abbreviation</b>	<b>Description</b>
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

<b>Abbreviation</b>	<b>Description</b>
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

<b>Abbreviation</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application</b>	<b>Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
<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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
Select a Rental	Main rental photo	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Main rental photo (low resolution)	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Photo of host	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Photo 2 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Photo 3 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Photo 4 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
Photo 5 of rental		<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Thumbnail photo of first reviewer	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Thumbnail photo of third reviewer	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	City	Set the city name.
	State/province	Set the state/province name.
	Country	Set the country name.
	Checkin date	Set the check-in date.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	Photo 4 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	Photo 5 of rental	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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>		

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Download File	Downloaded file name	Select an option: <ul style="list-style-type: none"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Get Public Link	Folder ID	Provide the folder ID.
Move File To Trash	N/A	N/A
View Trash	N/A	N/A

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
Game		
Logout	N/A	N/A
<i>eBanking</i>		
Sign Up	SignUp username	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	SignUp password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	SignUp confirm password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Login	Login username	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	Login password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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>		

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	Login password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	User password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Download Attachment	Download file	Select an option: <ul style="list-style-type: none"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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>		

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
<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:

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
		<ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
Student Load Homepage	Post attachment	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
View Submission	Submission document	Select an option: <ul style="list-style-type: none"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	Submission document webp format	Select an option: <ul style="list-style-type: none"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	User password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li></ul>

Application Action	Action Parameters	Parameter Description
		<ul style="list-style-type: none"> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
Replace Image	Username	Provide the username.
	File attachment	Select an option: <ul style="list-style-type: none"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to</li></ul>

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
		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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Logout of Google	User email address	Provide the user email address.
	Full user name	Provide the username.
<i>HTTP</i>		

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"> <li>• Accept-Language</li> <li>• Sec-Fetch-User</li> <li>• Upgrade-Insecure-Requests</li> <li>• Sec-Fetch-Site</li> </ul> <p>Use the <b>Add</b> button to add new options or the <b>Delete</b> 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"> <li>• Cache-Control</li> <li>• Etag</li> </ul> <p>Use the <b>Add</b> button to add new options or the <b>Delete</b> to remove them.</p>
	Response body	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> <li>• <b>Dynamic payload</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>

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"> <li>• Sec-Fetch-User</li> <li>• Upgrade-Insecure-Requests</li> <li>• Accept-Language</li> <li>• Sec-Fetch-Site</li> </ul> <p>Use the <b>Add</b> button to add new options or the <b>Delete</b> to remove them.</p>
	Request body	<p>Select an option:</p> <ul style="list-style-type: none"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> <li>• <b>Dynamic payload</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
	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"> <li>• Etag</li> <li>• Cache-Control</li> </ul> <p>Use the <b>Add</b> button to add new options or the <b>Delete</b> to remove them.</p>
	Response Body	Add a response message.

*Jingdong*

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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	User password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	User password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	User password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	Attachment filename	Provide the file name.
Open Message	N/A	N/A
Delete Message	N/A	N/A

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	User password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Logout	N/A	N/A
<i>Reddit</i>		
Load Main Page	N/A	N/A

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
<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.

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
	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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	Login password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
		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"> <li>• <b>Synthetic data (bytes)</b> and set the value.</li> <li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li> </ul>
Search Log	Index	Provide the index.
Logout	Username	Provide the user name.
<i>Tubi</i>		
Open Tubi Page	N/A	N/A

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
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"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
	Login password	Select an option: <ul style="list-style-type: none"><li>• <b>User input</b> and provide the value.</li><li>• <b>Playlist file</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
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"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Upload Video	Uploaded file name	Provide the file name.
	Uploaded file	Select an option: <ul style="list-style-type: none"><li>• <b>Synthetic data (bytes)</b> and set the value.</li><li>• <b>Payload profile</b> - select an option from the drop-down list or use the <b>Upload</b> button to upload a file.</li></ul>
Delete Video	N/A	N/A

<b>Application Action</b>	<b>Action Parameters</b>	<b>Parameter Description</b>
Like Video	N/A	N/A
Unlike Video	N/A	N/A
Logout	N/A	N/A
<b>Vkontakte</b>		
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
<b>Yammer</b>		
Select First Group	User email address	Provide the email address.
	User name	Provide the user name.
Select Second Group	User email address	Provide the email address.
Select Third Group	User email address	Provide the email address.
Like an Entry	User email address	Provide the email address.
Reply to a Post	User email address	Provide the email address.
	User name	Provide the user name.
Post New Message	User email address	Provide the email address.
	User name	Provide the user name.
Select Another Group	User email address	Provide the email address.

Application Action	Action Parameters	Parameter Description
<i>YYLive</i>		
Load Home Page	N/A	N/A
Select Category	Category	Provide the category.
Play Video	Video ID	Provide the Video ID.

### The difference between Dynamic and Payload files

- If the chosen file is Payload (not Dynamic), the exact contents of the file can be seen on the wire.
- If the chosen file is Dynamic and the file does not contain Macros, then the behavior is the same as above.
- If the chosen file is Dynamic and the file contains Macros, then each Macro is evaluated during the test with the expected value that the Macro is meant to generate.

## Artifacts

This section contains useful information and details on Playlist and Macro features.

### Rules and Grammar for Playlists

Rules to support comma or double-quotes as a part of a playlist:

1. Each playlist item with comma or double-quote in the content **must** be enclosed within double-quotes.
2. Every double-quote used as a part of the content must be escaped with another double-quote.

Each record is located on a separate line, delimited by a line break (CRLF). For example: `record = value * (COMMA value)` :

Record	value 1	value 2
abcd	abcd	
abcd,wxyz	abcd	wxyz
"abcd,pqr","wxyz"	abcd,pqr	wxyz
"abcd,pq""r","wxyz"	abcd,pq"r	wxyz

For all applications that have a **Sign In** or **Sign Up** action, the following parameters offer the possibility of uploading a playlist file: Login Username, Login password or SignUp Username, SignUp password, SignUp confirm password. Select the **Playlist file** option and select the **Upload** option:

The screenshot shows the 'Traffic Profiles (1 application)' configuration screen. On the left, there's a sidebar for 'Traffic Profile Configuration' with 'Predefined Applications' and a 'Applications' section. The main area has tabs for 'Actions' and 'Properties'. In the 'Actions' tab, there's a table with columns for '#', 'Name', and 'Weight'. One row is selected with the name 'eBanking Chrome to Apache 1'. In the 'Properties' tab, under 'Login username', there's a dropdown set to 'Playlist file' with a file selector. A red circle highlights the 'Upload' button. Below it, there's a 'Login password' field with 'User input' selected and the value 'user1pass'.

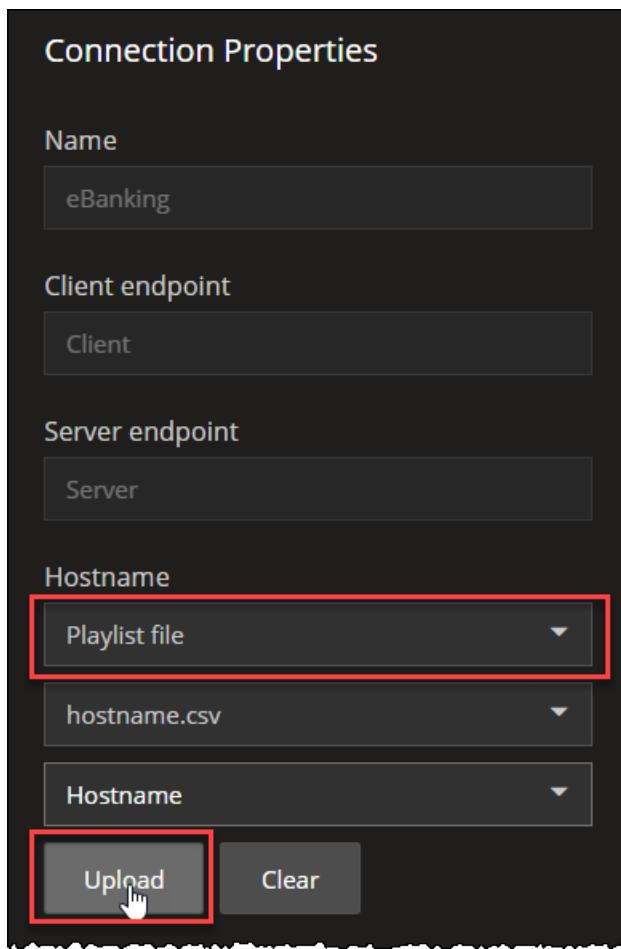
After the upload is performed, the reference column has corresponding csv column names, which can be chosen from the dropdown menu:

This screenshot shows the same interface after a CSV file has been uploaded. In the 'Actions' table, the 'Username' column now has a dropdown menu open, with 'Username' highlighted by a red box. Other options in the dropdown include 'Password' and 'Login password'. The rest of the interface remains the same as the first screenshot.

For some applications, the Hostname (under **ConnectionProperties**) offers the possibility of uploading a playlist file:

1. Select the **Playlist** file option .
2. Select **Upload**.

3. Choose the **Reference** column name from the drop-down.



Example of a Hostname playlist file:

**NOTE**

As of now, we do not validate empty Hostname values, if they are fetched from a playlist file.

	A	B
1	Hostname	
2	server1.com	
3	server2.com	
4	server3.com	
5	server4.com	
6	server5.com	
7	server6.com	
8	server7.com	
9	server8.com	
10	server9.com	
11	server10.com	
12		
13		
14		
15		
16		
17		

hostname(4107)

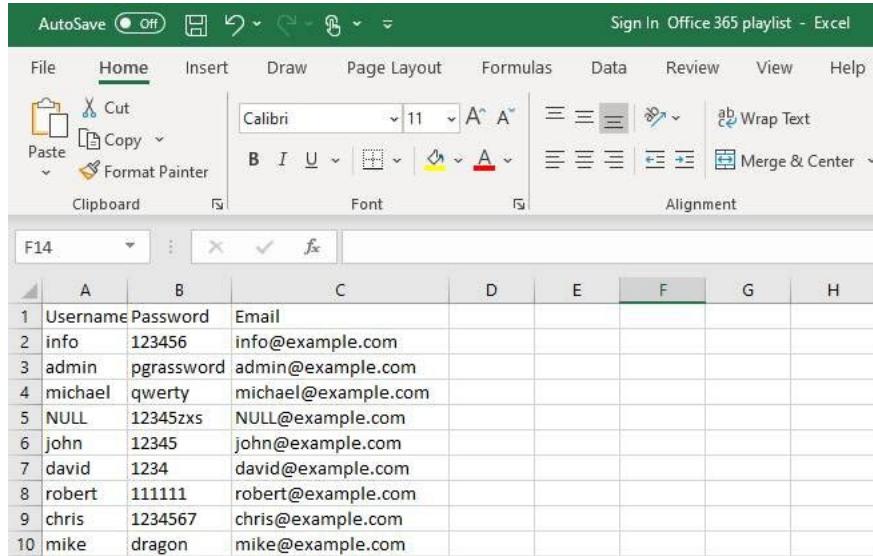
## About Playlists

For the **Sign In** action in eBanking, eShop, Social Network, Portal or the **Sign Up** action in eBanking applications, please use this [Sign In playlist](#) file:

Sign In playlist - Excel

	A	B	C	D	E	F	G	H	I
1	Username	Password							
2	admin	pgrassword							
3	michael	qwerty							
4	NULL	123456789							
5	john	12345							

For the **Sign In** action in Office 365 (Outlook, Excel, OneDrive) applications , please use this [Sign In Office 365 playlist](#) file:



The screenshot shows a Microsoft Excel spreadsheet titled "Sign In Office 365 playlist - Excel". The table contains 10 rows of data with columns labeled A through H. Column A is "Username", column B is "Password", and column C is "Email". The data is as follows:

	Username	Password	Email				
1	info	123456	info@example.com				
2	admin	pgrassword	admin@example.com				
3	michael	qwerty	michael@example.com				
4	NULL	12345zxs	NULL@example.com				
5	john	12345	john@example.com				
6	david	1234	david@example.com				
7	robert	111111	robert@example.com				
8	chris	1234567	chris@example.com				
9	mike	dragon	mike@example.com				
10							

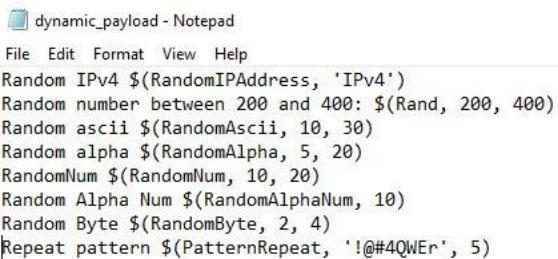
## About Macros

A macro is a method or function which allows you to customize the payload text data with the following parameters. The `maxLength` limit is set to 1024:

<b>Macros</b>	<b>Description</b>
<code>\$(RandomIPAddress, 'IPv4')</code>	The <b>RandomIPAddress</b> macro randomly generates IPv4 address. IPv6 is not yet supported.
<code>\$(Rand, minValue, maxValue)</code>	The <b>Rand</b> 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 <b>RandomAscii</b> 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 <b>RandomAlpha</b> 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 <b>RandomNum</b> 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 <b>RandomAlphaNum</b> macro generates a sequence of random letters or digits [A-Za-z0-9]. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.

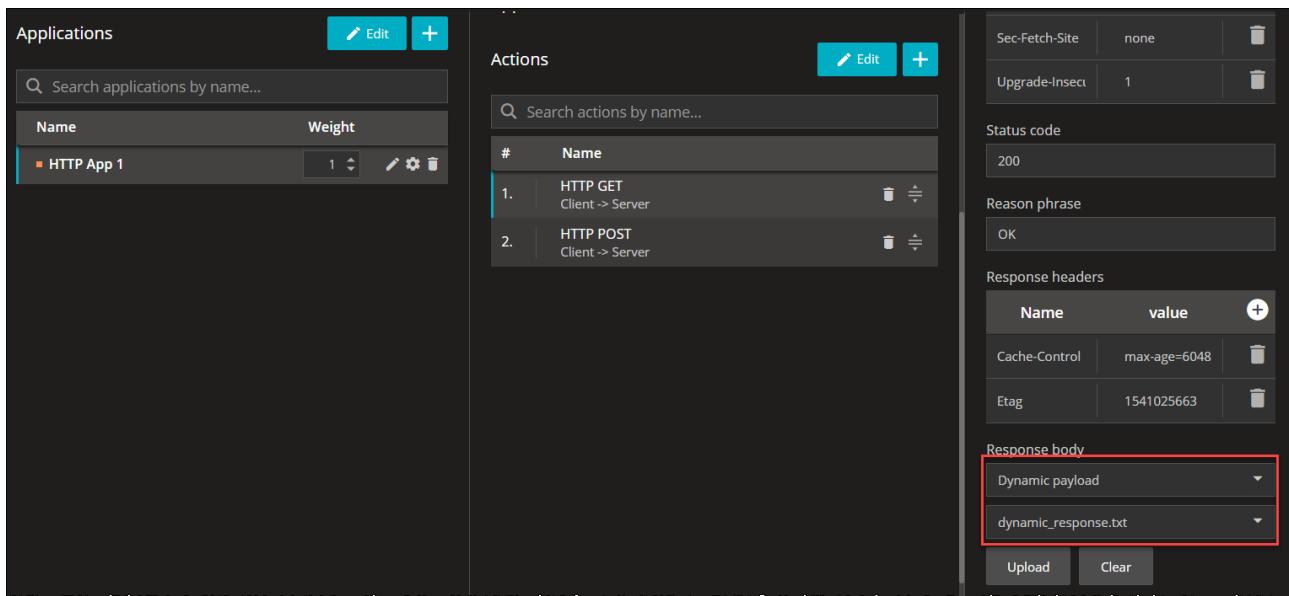
\$(RandomByte, minLength, maxLength)	The <b>RandomByte</b> macro generates a sequence of random bytes. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length.
\$(PatternRepeat, pattern, minLength, maxLength)	The <b>PatternRepeat</b> macro generates a sequence of characters by repeating the <pattern> pattern. minLength and maxLength are numbers. The sequence length is randomly chosen between the 2 values. If only one argument is specified, it is used as a fixed length. If the chosen length is not an exact multiple of the length of <pattern>, the last repetition of <pattern> is truncated.

The following is the macro file structure, and please use this [macros](#) file for the correct file format:



```
dynamic_payload - Notepad
File Edit Format View Help
Random IPv4 $(RandomIPAddress, 'IPv4')
Random number between 200 and 400: $(Rand, 200, 400)
Random ascii $(RandomAscii, 10, 30)
Random alpha $(RandomAlpha, 5, 20)
RandomNum $(RandomNum, 10, 20)
Random Alpha Num $(RandomAlphaNum, 10)
Random Byte $(RandomByte, 2, 4)
Repeat pattern $(PatternRepeat, '!@#4QWEr', 5)
```

This feature is also available for the HTTP application, on both HTTP GET and HTTP POST actions, under the following parameters: Response body/Response body. Switch to the dynamic payload and upload the `dynamic_payload` file:



The screenshot shows the ZAP interface with three main panels:

- Applications** panel: Shows a single application named "HTTP App 1" with a weight of 1.
- Actions** panel: Shows two actions: "HTTP GET Client -> Server" and "HTTP POST Client -> Server".
- Configuration Panel** (on the right):
  - Headers**: Sec-Fetch-Site: none, Upgrade-Insect: 1
  - Status code**: 200
  - Reason phrase**: OK
  - Response headers**: Cache-Control: max-age=6048, Etag: 1541025663
  - Response body** (highlighted with a red box):
    - Dynamic payload
    - dynamic\_response.txt

Assign the agents, enable capture and start the test. After the test is finished, download the captured information and you can see the payload, as set in the macro file:

No.	Time	Source	Destination	Protocol	Length	Info
16	0.099346	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 48737 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983045 TSecr=807789105
17	0.099359	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 37775 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983119 TSecr=807784865
18	0.099366	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 58394 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983026 TSecr=807847657
19	0.099374	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
20	0.099378	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
21	0.099378	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
22	0.099623	192.168.10.90	192.168.10.91	HTTP	590	HTTP/1.1 200 OK (text/plain)
23	0.099624	192.168.10.90	192.168.10.91	HTTP	602	HTTP/1.1 200 OK (text/plain)
24	0.099646	192.168.10.91	192.168.10.90	TCP	66	[TCP Window Update] 36116 → 80 [ACK] Seq=1 Ack=1 Win=2896 Len=0 TSval=764983171 TSecr=807846794
25	0.099651	192.168.10.91	192.168.10.90	HTTP	371	GET /file.txt?name1=val1 HTTP/1.1
26	0.099685	192.168.10.90	192.168.10.91	HTTP	582	HTTP/1.1 200 OK (text/plain)

> Frame 22: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits)  
> Ethernet II, Src: VMware\_A6:29:b9 (00:0c:29:a6:29:b9), Dst: VMware\_99:5a:02 (00:0c:29:99:5a:02)  
> Internet Protocol Version 4, Src: 192.168.10.90, Dst: 192.168.10.91  
> Transmission Control Protocol, Src Port: 80, Dst Port: 58394, Seq: 1, Ack: 306, Len: 524  
> Hypertext Transfer Protocol  
Line-based text data: text/plain (12 lines)  
Random IPv4 158.243.103.228\r\n  
Random number between 200 and 400: 266\r\n  
Random ascii \016\035EY\023Te1.'\]:\034+?\031p\*\026qI\030\024<\r\n  
Random alpha VEKzKn\r\n  
RandomNum 227499253664034\r\n  
Random Alpha Num RDtTu0rLmL\r\n  
Random Byte Y♦\r\n  
Repeat pattern !@#4QWEr!@#4QWEr!@#4QWEr!@#4QWEr!\r\n  
\r\n  
\r\n  
\r\n

# Index

---

**#**  
5G-EIR, configuration settings 558

**A**

agents  
  clear ownership 67  
  management 65  
  Network Management window 68  
  ownership 63  
  reboot 67  
  status of 65  
  tags 67

AMF, configuration settings 280

application traffic generator 214, 239, 242-243, 258, 343, 799, 824, 827, 841, 899, 950, 953, 1085, 1103, 1106, 1121, 1156

AUSF, configuration settings 301, 706

**B**

bidirectional UDP traffic flow 216, 801, 929, 1087

**C**

create/delete PDU session, secondary objective 203, 1080  
create/delete QoS Flows, secondary objective 201, 791, 1078

customer assistance 3

**D**

discovery, NRF 563  
DN, configuration settings 872  
DNN settings  
Full Core tests 127, 1008

SBA tests 663

**E**

enter/exit idle, secondary objective 200, 790, 1077  
EPS fallback 434, 1169

**F**

Full Core tests  
  configuration settings 111  
  global settings 120, 1002  
  network slicing 185, 1067  
  objectives 189, 1069

**H**

handover, secondary objective 788

**I**

IPFilterRule 764

**M**

middleware VM, upgrade 46  
modify QoS Flows, secondary objective 791

**N**

Network Management window 68  
Nnrf\_NFDiscovery 563  
NRF discovery 563  
NRF, configuration settings 395, 716

**O**

objectives  
  Full core tests 189, 1069  
  SBA tests 591  
  UPF Isolation tests 783

---

**P**

packet filters  
for SDF 764  
packet filter list configuration 141, 670, 1020  
Paging, secondary objective 199, 789, 1076  
passthrough testing 1271  
passwords  
admin, change 26  
PCF, configuration settings 413, 728  
product support 3

**Q**

QoS flows, settings 137, 1016

**R**

RadiusServer, configuration settings 275  
RAN, configuration settings 426, 851, 1162

**S**

SBA tests  
configuration settings 566  
global settings 658  
network slicing 584  
objectives 591  
SCP configuration settings 463, 734  
SGW-U, configuration settings 544  
SMF, configuration settings 486, 855  
SMS, secondary objective 204, 1081  
stateless UDP traffic generator 212, 322, 877, 926, 1083, 1135  
statistics  
licensing stats 1241

**T**

tags  
custom 67  
TCP connection settings 660

---

technical support 3

traffic generators 206, 321, 796, 876, 1082, 1134

**U**

UDM, configuration settings 518, 744  
UDP stateless, traffic generator 212, 322, 877, 926, 1083, 1135  
UDR, configuration settings 537, 751  
UE configuration settings  
Full Core tests 153, 1031  
SBA tests 571  
UPF Isolation tests 774  
UPF Isolation tests  
configuration settings 756  
global settings 758  
objectives 783  
UPF, configuration settings 544, 861  
URRs 765



© Keysight Technologies, 2019–2025

This information is subject to change  
without notice.

[www.keysight.com](http://www.keysight.com)