NSP
Network Services Platform
Release 26.4

System Administrator Guide

3HE-29840-AAAA-TQZZA
Issue 4
September 2026

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2026 Nokia.

Contents

About this document **19**

Part I: NSP administration basics **21**

1 NSP administration overview **23**

1.1 What does NSP administration involve? **23**

1.2 What is onboarding? **23**

1.3 What do I need to know about NSP licensing? **24**

1.4 How do I install the NSP license? **25**

1.5 How do I update the NSP license from Release 25.x to 26.4 or later? **26**

1.6 How do I view license points allocated to each NE? **28**

1.7 What do I need to know about extended NE software support for the NSP license? **29**

1.8 How do I receive product and documentation alerts? **30**

1.9 How do I view technical-support alerts? **30**

2 NSP access and UI administration **33**

2.1 What is NSP access administration? **33**

2.2 How do I enable single-address DR NSP system access? **35**

2.3 How do I configure NSP system settings? **36**

2.4 How do I configure alarm-severity colors? **37**

2.5 How do I customize the main menu? **38**

2.6 How do I configure linked URLs? **39**

2.7 How do I configure event logging? **40**

2.8 How do I configure an e-mail server for notifications? **41**

3 Map layout **45**

3.1 What is the Map Layout? **45**

3.2 Pathway: create and configure a physical Map Layout **50**

3.3 Pathway: create and configure an IGP Map Layout **50**

3.4 How do I create a physical Map Layout? **51**

3.5 How do I create an IGP Map Layout? **52**

3.6 How do I create a region for a physical Map Layout? **53**

3.7 How do I create a region for an IGP Map Layout? **54**

3.8 How do I place a region on the Map Layout? **55**

3.9 How do I create a zone in the Map Layout? **56**

3.10 How do I associate NEs or routers with a region? **57**

3.11 How do I add NEs to a zone? **58**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.12 How do I move connector objects in the Map Layout? 59
3.13 How do I enable GEO positioning for NEs and routers? 59
3.14 How do I rename the Map Layout? 60
3.15 How do I move an object to a specific GEO location? 61
3.16 How do I search for objects in the Map Layout? 62
3.17 How do I cancel un-deployed changes to the Map Layout? 63
3.18 What are best practices when using the Map Layout? 63

4 Resource pool management 65
4.1 How are resource pools used with programmable functions? 65
4.2 How do I search for a resource pool? 65
4.3 How do I view summary information for a resource pool? 66
4.4 How do I configure an IP address pool? 67
4.5 Why use IPv4 subnet re-purposing? 68
4.6 How do I configure a string pool? 68
4.7 How do I configure an RD-RT pool? 69
4.8 How do I configure a Numeric pool? 70
4.9 What are threshold policies? 71
4.10 How do I configure a threshold policy? 72
4.11 How do I reserve resources? 73
4.12 How do I release a resource? 74
4.13 How do I commit a resource? 75

5 NSP File Server 77
5.1 What is the NSP File Server? 77
5.2 File purge policies 77
5.3 How do I use the NSP File Server? 78
5.4 How do I configure file purge policies? 82

Part II: NSP security administration 85

6 SELinux administration 87
6.1 Overview 87
Deploying SELinux 88
6.2 What is SELinux? 88
6.3 How do I enable SELinux on an NSP deployer VM? 89
6.4 How do I enable SELinux in an NSP cluster? 91

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

SELinux for Classic Management **95**
6.5 What does enabling NFM-P SELinux involve? **95**
6.6 How do I enable SELinux on the NFM-P? **95**
6.7 How do I enable SELinux enforcing mode for the NFM-P? **100**
SELinux troubleshooting **103**
6.8 What does NSP SELinux troubleshooting involve? **103**
6.9 How do I switch between SELinux modes on NSP system components? **103**
6.10 How do I troubleshoot SELinux on NSP system components? **105**
6.11 How do I troubleshoot SELinux on the NFM-P? **107**

7 TLS administration **111**
7.1 Overview **111**
What is NSP TLS administration? **113**
7.2 NSP TLS administration overview **113**
7.3 Managing Kubernetes infrastructure TLS **114**
7.4 Managing NSP system TLS **115**
NSP Kubernetes TLS administration procedures **116**
7.5 How do I update the K3s certificate for an NSP deployer VM? **116**
7.6 How do I update the Kubernetes registry TLS certificate? **117**
7.7 How do I update nsp_kubeconfig on the NSP deployer host? **119**
7.8 How do I add Kubernetes load balancer external IP addresses? **119**
NSP cluster TLS administration procedures **121**
7.9 How do I list the NSP Kubernetes secrets? **121**
7.10 How do I view the Kubernetes secret content? **122**
7.11 How do I update the NSP issuer TLS certificates? **123**
7.12 How do I update the custom NSP server TLS certificates? **127**
7.13 How do I add an NSP Kubernetes secret? **130**
7.14 How do I recreate the NSP Kubernetes secrets? **132**
7.15 How do I back up the NSP Kubernetes secrets? **138**
7.16 How do I restore the NSP Kubernetes secrets? **139**
7.17 How do I update the Keycloak OpenSearch client secret? **140**
NSP component TLS configuration **142**
7.18 How do I configure an NSP auxiliary database to request the NSP TLS certificate? **142**
7.19 How do I configure an NFM-P main server to request the NSP TLS certificate? **143**
7.20 How do I configure an NFM-P auxiliary server to request the NSP TLS certificate? **146**
7.21 How do I enable TLS for NFM-P XML API clients? **149**
7.22 How do I disable TLS for NFM-P XML API clients? **152**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8 NSP user security **155**
User management **155**
8.1 What is user management? **155**
8.2 What are the NSP user management requirements and restrictions? **156**
8.3 How do I configure an NSP user? **159**
8.4 How do I import users and groups from NFM-P? **162**
8.5 How do I set global user session limits? **164**
8.6 What are user password policies? **165**
8.7 How do I set local user password requirements? **166**
8.8 How do I set login protection restrictions? **168**
8.9 How do I suspend a user account? **169**
8.10 How do I configure user account event notifications? **170**
8.11 How do I configure a remote authentication server? **171**
8.12 Remote authentication server parameters **173**
8.13 How do I configure a remote identity provider? **175**
8.14 How do I configure a direct URL to NSP for IDP users? **178**
NSP User Access Control **179**
8.15 What is User Access Control? **179**
8.16 Pathway: Configure User Access Control **181**
8.17 How do I configure alarm access using roles? **182**
8.18 How do I configure a role? **184**
8.19 How do I set network resource access levels? **186**
8.20 How do I configure a user group? **188**
8.21 How do I configure a default user group? **189**
8.22 How do I configure user access in Log Viewer? **189**
8.23 How do I enable User Access Control? **190**
8.24 What are NSP operator roles and responsibilities? **191**
8.25 How do I update the NSP TLS certificate for remote authentication? **194**
User session management and logging **196**
8.26 What is user session management? **196**
8.27 How do I terminate user sessions? **196**
8.28 How do I send a message to active users? **197**
8.29 How do I view user events? **198**
8.30 How do I filter the event log view? **199**
8.31 How do I apply or clear my advanced filters? **200**
8.32 How do I modify my advanced filters? **200**
8.33 How do I set the User Activity Log to auto-refresh? **201**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.34 How do I set limits for log event retention? 202
8.35 How do I export activity log events? 203
Network resource groups 205
8.36 What are group directories and resource groups? 205
8.37 Pathway: create group directories and resource groups 205
8.38 How do I create a group directory? 205
8.39 How do I configure a resource group? 206
8.40 How do I associate a resource group with a group directory? 208
8.41 How do I search for a management object? 209
Kafka authorization 210
8.42 What is Kafka authorization? 210
8.43 How do I enable Kafka authorization? 212

9 Classic management security 215
Securing NFM-P system access 215
9.1 What is NFM-P system security? 215
9.2 How do I change an NFM-P main database password in a standalone system? 215
9.3 How do I change an NFM-P main database password in a redundant system? 218
9.4 How do I update the supported NFM-P TLS versions and ciphers? 223
NFM-P user security 231
9.5 What is NFM-P user security? 231
9.6 How do I manage NFM-P user accounts and groups? 232
9.7 What is user activity logging? 236
9.8 How do I configure sample span rule? 241
9.9 Pathway: configure and manage NFM-P user security 242
9.10 How do I reserve an admin account login? 244
9.11 How do I create a scope of command role? 245
9.12 How do I create a scope of command profile? 246
9.13 How do I create a span of control? 247
9.14 How do I create a span of control profile? 248
9.15 How do I create a span rule? 248
9.16 How do I create an NFM-P user group? 249
9.17 How do I add or remove workspaces for a user group? 250
9.18 How do I create an NFM-P user account? 252
9.19 How do I copy an NFM-P user account? 253
9.20 How do I configure global user account and password expiry? 254
9.21 How do I configure the GUI client inactivity timeout? 255

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.22 How do I configure the minimum allowable user name length? 255
9.23 How do I configure authentication failure actions? 256
9.24 How do I configure suspended account actions? 256
9.25 How do I configure automated E-mail notification? 257
9.26 How do I list inactive user accounts? 258
9.27 How do I suspend or reinstate an NFM-P user account? 258
9.28 How do I change an NFM-P user password? 259
9.29 How do I update NSP XML API user access details? 260
9.30 How do I disable an NFM-P user password? 261
9.31 How do I change the password of the current NFM-P user? 262
9.32 How do I export the local tab preferences of one or more users? 262
9.33 How do I assign local tab preferences to users? 263
9.34 How do I send a broadcast message to GUI clients? 264
9.35 How do I view and manage the active GUI client sessions? 265
9.36 How do I disconnect an XML API JMS client connection or remove a durable subscription? 266
9.37 How do I view the user activity log? 267
9.38 How do I view the user activity associated with an object? 268
9.39 How do I change the maximum number of concurrent NFM-P admin operator positions? 269
9.40 How do I configure the number of allowed client sessions for a client delegate server? 270
9.41 How do I change the NFM-P Task Manager settings? 271
9.42 How do I export all workspaces and local tab preferences? 273
9.43 How do I import workspaces and local tab preferences? 273

10 Classic management NE security 275
10.1 What is NFM-P NE security? 275
10.2 What are RADIUS, TACACS+, and LDAP? 276
10.3 What is device SSH security? 277
10.4 How do I restore support for disabled NE SSH algorithms? 277
10.5 What are CPM filters and traffic management? 280
10.6 What is DoS protection? 281
10.7 What is DDoS protection? 282
10.8 What is IP security? 284
10.9 HSM 284
10.10 Pathway: manage NE user and device security 285
10.11 How do I configure a MAF? 287
10.12 How do I configure a CPM filter? 288
10.13 How do I configure an NE DoS protection policy? 291

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.14 How do I view NE DoS protection violations? 292
10.15 How do I configure an NE DDoS protection policy? 293
10.16 How do I configure NE TLS client authentication? 295
10.17 How do I configure NE TLS server authentication? 298
10.18 How do I configure TLS server group list? 299
10.19 How do I configure TLS client group list? 300
10.20 How do I configure TLS server signature list? 301
10.21 How do I configure TLS client signature list? 301
10.22 How do I configure a site user profile? 302
10.23 How do I configure a user account on a managed device? 303
10.24 How do I configure an NE password policy? 304
10.25 How do I configure an LDAP site authentication policy? 305
10.26 How do I configure an NE RADIUS authentication policy? 306
10.27 How do I configure an NE TACACS+ authentication policy? 308
10.28 How do I configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy? 309
10.29 How do I configure device system security settings? 310
10.30 How do I configure and manage PKI site security on an NE? 313
10.31 How do I configure a PKI certificate authority profile? 316
10.32 How do I configure the automatic renewal of the PKI certificate? 317
10.33 How do I configure a PKI common name list? 319
10.34 How do I configure an Enrollment over Secure Transport profile? 320
10.35 How do I add an HSM to the NFM-P? 321
10.36 How do I create a file transmission profile? 322
10.37 How do I perform CMPv2 actions? 322
10.38 How do I delete a security policy? 325
10.39 How do I manually unlock a user account? 326
10.40 How do I clear the password history of a user on a managed device? 327
10.41 How do I clear collected statistics on a CPM filter? 327
10.42 How do I manage OCSP cache entries on an NE? 329
10.43 What is TCP enhanced authentication? 330
10.44 Pathway: configure TCP enhanced authentication for NEs 331
10.45 How do I configure a global TCP key chain? 332
10.46 How do I distribute global key chains to NEs? 333
10.47 How do I verify the distribution of a global key chain to NEs? 334
10.48 How do I identify differences between a global and local key chain policy or two local key chains? 335

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part III: NSP system administration **337**

11 NSP system configuration and management **339**

11.1 What is NSP system configuration and management? **339**
11.2 How do I change the nsp user password? **339**
11.3 How do I add an NSP feature package? **340**
11.4 How do I update the NSP system configuration? **340**
11.5 How do I regenerate an NSP system token? **342**
11.6 PKI server access **344**
11.7 How do I change the NSP cluster registry password? **344**
11.8 How do I remove the stale NSP allowlist entries? **345**
11.9 How do I disable NSP websocket event notifications? **347**
11.10 How do I install custom Mistral actions for NSP Workflows? **348**
11.11 How do I remove Mistral actions from NSP? **350**
11.12 How do I configure a generic mediator? **351**
11.13 How do I configure an NSP Workflows trigger framework? **354**
11.14 How do I manage NSP Analytics logging? **356**
11.15 How do I resynchronize Analytics data dictionary objects? **357**
11.16 How do I verify disk performance for etcd? **358**
11.17 What are OpenSearch audit logs? **360**
11.18 How do I enable OpenSearch audit logging? **360**
11.19 How do I view OpenSearch audit logs? **362**

12 NSP cluster administration **363**

NSP cluster control and operation **363**

12.1 How do I manage NSP clusters? **363**
12.2 How do I view the status of all Kubernetes pods? **363**
12.3 How do I retrieve pod information? **364**
12.4 How do I retrieve a list of cluster members? **365**
12.5 How do I retrieve cluster member information? **365**
12.6 How do I change internal user account names and passwords? **367**
12.7 Pathway: stop and start DR NSP clusters **368**
12.8 How do I stop an NSP cluster? **371**
12.9 How do I start an NSP cluster? **373**
12.10 How do I switch an NSP cluster between SELinux modes? **374**
12.11 How do I identify the control-planes in an NSP cluster? **375**
12.12 How do I display the NSP cluster status? **376**
12.13 How do I restart a Kubernetes pod? **377**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.14 How do I delete Errored or Evicted pods? 378
12.15 How do I recover pods in CrashLoopBackOff state? 379
NSP cluster lifecycle management 383
12.16 What is Kubernetes cluster lifecycle management? 383
12.17 How do I move a Kubernetes pod to a different node? 383
12.18 How do I add an NSP cluster node? 385
12.19 How do I remove an NSP cluster node? 388
12.20 How do I change NSP system addressing? 390
12.21 How do I back up the NSP deployer VM? 391
12.22 How do I restore the NSP deployer VM? 392
12.23 How do I replace an NSP cluster node? 395
12.24 How do I restore the NSP OpenSearch log data? 402

13 NSP cluster database administration 405
13.1 How do I check NSP database synchronization? 405
13.2 What do I need to know about backing up and restoring NSP cluster data? 407
13.3 How do I configure scheduled NSP backups? 408
13.4 How do I back up the NSP cluster databases? 410
13.5 How do I retrieve cluster database backup files? 413
13.6 How do I restore the Kubernetes etcd data in an NSP cluster? 414
13.7 How do I restore the NSP cluster databases? 417
13.8 How do I recover a failed nsp-tomcat database in a DR NSP deployment? 424
13.9 How do I recover both failed nsp-tomcat databases in a DR NSP deployment using a database backup? 428
13.10 How do I recover both nsp-tomcat databases in a DR NSP deployment without a database backup? 434
13.11 How do I recover nsp-tomcat databases in an HA cluster? 439

14 NSP logging and monitoring 441
14.1 What is System Health? 441
14.2 What are the System Health functions? 441
14.3 What is Log Viewer? 442
14.4 What is Grafana? 443
14.5 What is user activity log forwarding? 444
14.6 What is the syslog record format for NSP application log forwarding? 445

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part IV: NSP disaster recovery **447**

15 Disaster recovery for NSP clusters **449**

15.1 What are the NSP cluster DR functions? **449**

15.2 Pathway: prepare for an NSP DR switchover **451**

15.3 How do I identify the NSP cluster DR roles? **452**

15.4 How do I perform an NSP DR switchover from the NSP UI? **453**

15.5 How do I display the NSP DR failover setting? **454**

15.6 How do I disable NSP DR failovers? **455**

15.7 How do I enable NSP DR failovers? **456**

16 Disaster recovery for NSP components **459**

16.1 What are the NSP component DR functions? **459**

16.2 What is auxiliary database redundancy? **459**

16.3 How do I perform an auxiliary database switchover? **460**

16.4 What is classic management redundancy? **463**

16.5 What are the NFM-P system redundancy models? **463**

16.6 What are the NFM-P redundancy functions? **467**

16.7 How do I respond to NFM-P redundancy failures? **474**

16.8 Pathway: manage NFM-P redundancy **478**

16.9 How do I view the NFM-P system redundancy status? **479**

16.10 How do I view the NFM-P auxiliary server status? **482**

16.11 How do I perform a server activity switch? **484**

16.12 How do I configure main database switchover behavior? **485**

16.13 How do I perform a main database switchover using the NFM-P client GUI? **486**

16.14 How do I perform a main database switchover using a CLI script? **487**

16.15 How do I enable or disable automatic database realignment? **488**

Part V: NSP component administration **493**

17 MDM administration **495**

17.1 What is MDM administration? **495**

17.2 What should I know about adaptor artifact management? **495**

17.3 How do I install artifacts that are not supported in the Artifacts view? **496**

17.4 How do I enable mTLS on the NSP mediation interface? **499**

17.5 How do I enable TLS and mTLS for telemetry and gNMI on_change support? **500**

17.6 How do I manage MDM model definitions? **503**

17.7 How do I manage MDM device mappings? **506**

17.8 How do I uninstall MDM adaptor suites? **508**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17.9 How do I restart an MDM server? 511
17.10 How do I retrieve detailed information about MDM servers? 512
17.11 How do I rebalance NE load on MDM servers? 514

18 Artifact administration 515
18.1 What is NSP artifact administration? 515
18.2 How do I create a public/private key pair? 516
18.3 How do I manage public/private key pairs? 518

19 Telemetry administration 519
19.1 What is telemetry administration? 519
19.2 Process to enable CN telemetry 519

20 NSP auxiliary database administration 521
20.1 What is an NSP auxiliary database? 521
20.2 How do I collect NSP log files? 523
20.3 How do I start an auxiliary database cluster? 523
20.4 How do I stop an auxiliary database cluster? 525
20.5 How do I check the auxiliary database status? 527
20.6 How do I change the samauxdb RHEL user password? 530
20.7 How do I schedule auxiliary database backups? 531
20.8 How do I manually backup the auxiliary database? 532
20.9 How do I check the auxiliary database backup status? 532
20.10 How do I restore an auxiliary database? 533
20.11 How do I change an auxiliary database user password? 541
20.12 How do I change the auxiliary database external IP addresses? 542
20.13 How do I test auxiliary database disk performance? 547
20.14 How do I add an auxiliary database station? 549
20.15 How do I replace an auxiliary database station? 561
20.16 How do I remove an auxiliary database station? 566
20.17 How do I recreate an auxiliary database? 574
20.18 How do I customize auxiliary database tables? 580
20.19 How do I create and manage custom auxiliary database table attributes in NFM-P? 583
20.20 How do I create and manage custom auxiliary database table attributes in NSP? 585

21 Classic management administration 589
NFM-P component administration 589
21.1 Pathway: redundant NFM-P shutdown and restart 589
21.2 How do I start a main server? 593

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.3 How do I stop a main server? 593
21.4 How do I start a main database? 594
21.5 How do I stop a main database? 595
21.6 How do I start an auxiliary server? 596
21.7 How do I stop an auxiliary server? 597
NFM-P administration and management 598
21.8 What is global NFM-P system configuration? 598
21.9 How do I change default text-field and ID ranges? 598
21.10 What are the system preferences configuration procedures? 603
21.11 How do I set the NFM-P system preferences? 603
21.12 How do I create or configure a format policy? 608
21.13 How do I create or configure a range policy? 610
21.14 How do I modify the base configuration of all GUI clients? 612
21.15 How do I change the default user file locations on a client delegate server? 613
21.16 How do I enable main database backup file synchronization? 614
21.17 How do I modify the default time period of statistics displayed by the Statistics Manager search filters? 616
21.18 How do I modify the default time period of statistics displayed on object properties forms? 617
21.19 How do I enable the preservation of the XML API statistics pool size? 618
21.20 How do I configure auto-assigned service ID ranges and uniqueness checking? 620
NFM-P alarm administration 623
21.21 What are alarm thresholds? 623
21.22 What is alarm suppression? 625
21.23 What is the alarm purge algorithm? 626
21.24 What is automatic deletion of correlated alarms? 627
21.25 What is alarm debouncing? 627
21.26 How do I filter alarms for XML API clients using the NFM-P GUI? 629
21.27 How do I configure alarm policies? 629
21.28 How do I configure alarm severity and deletion behavior? 631
21.29 How do I configure alarm history logging? 632
21.30 How do I show or hide the alarm Additional Text button? 633
21.31 How do I configure alarm debouncing ? 634
21.32 How do I configure alarm filters for XML API clients? 634
21.33 How do I reload all alarms from the historical alarm database? 636
21.34 How do I manually escalate or de-escalate the severity of an alarm on the NFM-P? 636
21.35 How do I optimize alarm event notifications? 637

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P license management **639**
21.36 What are NFM-P licenses? **639**
21.37 How do I view the NFM-P license information? **640**
21.38 How do I export the NFM-P license information or create a license point inventory? **641**
21.39 How do I update the NFM-P license in a standalone deployment? **641**
21.40 How do I update the NFM-P license in a redundant deployment? **642**
21.41 How do I list the backed-up NFM-P license files? **645**
21.42 How do I change the default NFM-P license expiry notification date? **646**
NFM-P network management configuration **648**
21.43 How do I configure implicitly clearing alarm behavior for node reboots? **648**
21.44 How do I configure backup-file retention for deleted NEs? **649**
21.45 How do I enable alarm reporting to identify duplicate NE system IP addresses? **651**
21.46 How do I enable dynamic system IP address updates for 7705 SAR nodes? **653**
21.47 How do I enable LSP on-demand resynchronization? **654**
21.48 How do I enable debug configuration file reloading on an NE for mirror services? **655**
21.49 How do I configure throttle rates for subscriber trap events? **657**
21.50 How do I configure the windowing trap delayer option for subscriber table resyncs? **658**
21.51 How do I create a default SNMPv2 OmniSwitch user? **660**
Setting NFM-P OLC states **662**
21.52 What is an OLC state? **662**
21.53 How do I display equipment or service OLC states? **664**
21.54 How do I display the OLC state change schedules? **664**
21.55 How do I change the OLC state of one or more objects? **665**
21.56 How do I lock the OLC state? **666**
21.57 How do I schedule an OLC state change? **667**
21.58 How do I change the OLC state assigned to one or more alarms? **667**
21.59 How do I add the OLC state property to a manually created service template? **668**
NFM-P platform modification and replacement **670**
21.60 What is platform modification? **670**
21.61 How do I test NFM-P disk performance? **671**
21.62 How do I relink the Oracle executable files? **674**
21.63 How do I change the IP address or hostname of an NFM-P component? **675**
NFM-P maintenance **677**
21.64 What is NFM-P system maintenance? **677**
21.65 How do I back up the main database? **682**
21.66 How do I collect and store NFM-P log and configuration files? **683**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Daily maintenance **684**
21.67 How do I check the main database performance? **684**
21.68 How do I back up the NFM-P log and configuration files? **685**
Weekly maintenance **687**
21.69 How do I back up and restore NE configuration files? **687**
21.70 How do I check the NE scheduled backup status? **687**
21.71 How do I back up the NE configuration files? **689**
21.72 How do I restore the NE configuration files? **690**
21.73 Why collect device hardware inventory data? **691**
21.74 How do I collect port inventory data for a specific managed device? **691**
21.75 How do I manage main database audit logs? **693**
21.76 How do I reduce the number of Oracle audit logs? **693**
21.77 How do I check for performance monitoring statistics collection? **693**
Monthly maintenance **695**
21.78 Why generate and store a user account list? **695**
21.79 How do I generate and store user account data? **695**
21.80 How do I test an NFM-P main database restore? **696**
21.81 Why check the NFM-P platform performance? **700**
21.82 How do I check Windows client station performance? **701**
21.83 How do I check network connections between components? **702**
21.84 How do I measure NFM-P performance? **703**
21.85 How do I check network management connections? **704**
21.86 How do I test main server and database redundancy switches? **706**

22 Classic management database administration **707**
22.1 What is the NFM-P main database? **707**
22.2 How do I restore and reinstantiate the NFM-P main database? **709**
22.3 Pathway: NFM-P database management **710**
22.4 How do I view the main database properties? **712**
22.5 How do I configure the Oracle database user lockout threshold? **713**
22.6 How do I unlock the Oracle database user account? **715**
22.7 How do I configure Oracle database error monitoring? **716**
22.8 How do I configure a size constraint policy? **716**
22.9 How do I configure an ageout constraint policy? **718**
22.10 How do I create a database file policy to manage database log or core dump files? **719**
22.11 How do I configure the statistics data retention period for the main database? **721**
22.12 How do I back up the main database from the client GUI? **721**

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.13 How do I back up the main database from a CLI? 723
22.14 How do I schedule main database backups? 726
22.15 How do I restore a standalone main database? 727
22.16 How do I restore the primary main database in a redundant system? 735
22.17 How do I delete the inactive residential subscriber instances? 746
22.18 How do I export an NFM-P main database? 748
22.19 How do I import an NFM-P main database? 752
22.20 How do I reinstantiate the main database from the client GUI? 755
22.21 How do I reinstantiate the main database from a CLI? 756
22.22 How do I regenerate NSP TLS certificates for an NFM-P database? 758

A Remote authentication sample configurations 761
A.1 Remote authentication server configurations 761

B Classic management scope of command roles and permissions 771
B.1 What are the predefined NFM-P scope of command profiles and roles? 771
B.2 What are the permissions assignable to NFM-P scope of command roles? 774
B.3 What is the permissions access for NFM-P scope of command roles? 798

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

About this document

Purpose

The *NSP System Administrator Guide* is intended for operators who have NSP system administrator privileges and need to understand or perform Network Services Platform system management or maintenance. The guide describes how to perform operations for system and component configuration, security, access, and database management.

Scope

The scope of this document is limited to NSP system administration. Readers of the guide are advised to familiarize themselves with the different aspects of the administration process. Each part, chapter, or section describes a specific area of interest or administrative function.

Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to Documentation Feedback.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part I: NSP administration basics

Overview

Purpose

This part of the *NSP System Administrator Guide* introduces the document content and structure, and provides fundamental NSP administration information.

Contents

Chapter 1, NSP administration overview	23
Chapter 2, NSP access and UI administration	33
Chapter 3, Map layout	45
Chapter 4, Resource pool management	65
Chapter 5, NSP File Server	77

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1 NSP administration overview

1.1 What does NSP administration involve?

1.1.1 Guide description

The *NSP System Administrator Guide* describes how to perform various NSP management operations as requirements arise, or as directed by technical support.

The guide is written for an NSP operator who has the NSP administrator role assigned to their NSP user group.

1.1.2 NSP administrator responsibilities

An NSP system administrator can manage all NSP functional areas, and is primarily responsible for the following:

- basic, global GUI and operational configuration, as described in this part, Part I: “NSP administration basics”
- system security, such as TLS configuration and user management, as described in Part II: “NSP security administration”
- low-level system control and configuration, as described in Part III: “NSP system administration”
- fault tolerance administration, as described in Part IV: “NSP disaster recovery”
- control and configuration of ancillary NSP components, as described in Part V: “NSP component administration”

Note: It is strongly recommended that you perform an administrative procedure in this document only under the guidance of technical support.

1.2 What is onboarding?

1.2.1 Introduction

NSP includes an onboarding wizard that guides you through the initial setup of the NSP-managed network. During onboarding, you import artifacts required for node management, create discovery rules to scan the network, manage discovered nodes, configure map settings, enable statistics collection, and set up user accounts with the appropriate permissions.

Onboarding is performed once, typically by the system administrator.

Although onboarding applies to all deployments, the full procedure is found in the Enterprise Guide. See ”NSP Onboarding” in the *NSP Enterprise Guide* for complete onboarding instructions.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.3 What do I need to know about NSP licensing?

1.3.1 NSP licensing

Starting with NSP Release 25.4, the Centralized License Manager (CLM) is integrated within each NSP deployment. CLM is still offered as a standalone product to manage NE licenses in deployments without NSP; however, as of NSP Release 25.4, the CLM functions have been embedded in NSP and enhanced to handle NSP system licensing. The entitlements of the NSP system license key (which is called the NSP Routing key in NSP CLM) include information about license points and feature packages.

The information contained in this section specifically refers to the NSP-integrated deployment of CLM. For information about independent CLM deployment, consult the Centralized License Manager documentation, including the *CLM User Guide* and the *CLM Installation and Upgrade Guide*.

The NSP license key is added after NSP installation. Entitlements within the NSP license key can be added, viewed, and maintained over time from the Centralized License Manager option in the NSP main menu.

You only need one NSP license key for the NSP whether you have a standalone NSP setup, or whether you have an HA or HA/DR setup.

If you intend to run NSP Simulation in addition to NSP, the NSP Simulation needs to be installed in a separate cluster. This requires another unique NSP license key for NSP Simulation.

While Automation Packages (APs) appear in the license request form, they do not require an NSP license.

1.3.2 NSP license key expiry notifications

The NSP checks the expiry date of the NSP license key every time a new NSP web-UI tab is opened in the browser or once a day for a web-UI tab that is already logged into the NSP. It issues alarms and banners to notify the NSP user in advance of the NSP license expiry. After the NSP license key expires, the NSP continues to operate.

Alarms

Prior to the NSP license key expiration date, NSP issues daily alarms with increasing severity levels at 180, 90, and 7 days before expiration. These alarms can be viewed in the **Current Alarms** view as well as in **Centralized License Manager**, **Notifications**. For more details about specific alarms, see “What does this notification mean?" in the *Centralized License Manager User Guide*.

NSP raises the following alarms:

- minor alarm once every 24 hours starting 180 days prior to expiration
- major alarm issued every 24 hours starting at 90 days before expiration
- critical alarm 7 days before expiration and thereafter

Banners

The NSP issues banners in the NSP banner bar to notify users of the NSP license key expiry and provides information about actions that can be taken.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

In most cases, users will be notified about the NSP license key expiry; however, only administrators can contact Nokia Support to acquire a new NSP licence key.

- License key expiry in 180 days or less

  The notification only appears when the administrator is logged in. It can be closed and reappears on next login. The suggested action is to add a new NSP license key.

- License key expiry in 90 days or less

  The notification is visible to all users and can be closed. It reappears on next login.

  The suggested action for administrators is to add a new NSP license key; for other users it is to contact the administrator.

- License key expiry in 7 days or less

  The notification is visible to all users and cannot be closed.

  The suggested action for administrators is to add a new NSP license key; for other users it is to contact the administrator.

- Expired license key

  After the NSP license key is expired, the notification in the banner bar can no longer be closed by any users. Adding a new NSP license key clears this notification banner.

  The suggested action for administrators is to add a new NSP license key; for other users it is to contact the administrator.

- No license key

  If the NSP is installed without purchasing the necessary entitlements to manage the equipment, the NSP notifies users that the NSP licence key was not found. This notification is visible to all users and cannot be closed. Adding a new NSP license key clears the notification.

  The suggested action for administrators is to add a new NSP license key; for other users it is to contact the administrator.

1.4 How do I install the NSP license?

1.4.1 Purpose

Use this procedure to install your NSP license.

Note: This procedure applies to NSP license installation only. For NFM-P licensing, see “NFM-P license management” (p. 639).

1.4.2 Prerequisites

In order to install your NSP license, you must already have NSP installed or upgraded. This gives you access to the NSP CLM.

See “To install an NSP cluster” in the *NSP Installation and Upgrade Guide* to install NSP.

See “NSP system upgrade” in the *NSP Installation and Upgrade Guide* to upgrade NSP.

Once you have access to the NSP UI, follow the steps below.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.4.3 Steps

1

Open **Centralized License Manager** (CLM) from the NSP main menu.

2

From the view selector, select **Configurations**.

3

Download the **System Certificate Signing Request (CSR)**, which contains the system UUID and keys specific to your deployment.

NSP uses the same UUID for both active and standby instances. The same UUID is also used after switchover.

4

Email the license request to your Nokia representative to request an NSP license key (also known as the NSP Routing key). The request is for one UUID and consists of the downloaded file (zip archive) and the NSP routing options for your deployment.

In response, Nokia will prepare an Installation.zip containing all applicable NSP routing licenses, which can include nfmpLicense.xml, nspRoutingLicense.xml, and vsrnrcLicense.txt, depending on the NSP routing options selected in the license request.

5

Extract the Installation.zip file received from Nokia and upload the system license to NSP:

a. Open **Centralized License Manager, Network Pool Keys** and click **+ Pool Key**.

b. Choose the file that contains the NSP Routing key (nspRoutingLicense.xml) and click **Upload**.

6

Optionally, upload any other license files you received from Nokia.

END OF STEPS

1.5 How do I update the NSP license from Release 25.x to 26.4 or later?

1.5.1 Purpose

Use this procedure to update your NSP license from NSP Release 25.x to 26.4 or later.

Starting with NSP Release 26.4, you must have an NSP license that includes the NSP Developer feature package if you intend on using customer-created or modified workflows, intents, or adaptors. See *NSP System Architecture Guide* for more information about feature packs and what is included in the NSP Developer feature package.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: This procedure does not apply if you are updating your NSP license from pre-NSP 25 releases directly to NSP Release 26.

Note: This procedure applies to NSP license update only. For NFM-P licensing, see “NFM-P license management” (p. 639).

Note: If the NSP license is not updated, using customer-created workflows, intents, or adaptors may cause them to not execute and trigger the following alarm: EntitlementResourceAlert; see 1.7.2 “ What does this alarm mean?” (p. 29).

1.5.2 Prerequisites

In order to update your NSP license from NSP Release 25.x to 26 or later, you must already have NSP Release 25 installed or upgraded. This gives you access to the NSP CLM.

Note: Do not yet upgrade the NSP Release 25.x to 26 or later until prompted to do so in Step 5.

1.5.3 Steps

1

Open **Centralized License Manager** (CLM) from the NSP main menu.

2

From the view selector, select **Configurations**.

3

Download the **System Certificate Signing Request (CSR)**, which contains the system UUID and keys specific to your deployment.

NSP uses the same UUID for both active and standby instances. The same UUID is also used after switchover.

4

Email the license request to your Nokia representative to request an NSP license key (also known as the NSP Routing key). The request is for one UUID and consists of the downloaded file (zip archive) and the NSP routing options for your deployment.

In response, Nokia will prepare an Installation.zip containing all applicable NSP routing licenses, which can include nfmpLicense.xml, nspRoutingLicense.xml, and vsrnrcLicense.txt, depending on the NSP routing options selected in the license request.

5

Upgrade NSP from Release 25 to 26.

See “To install an NSP cluster” in the *NSP Installation and Upgrade Guide* to install NSP.

See “NSP system upgrade” in the *NSP Installation and Upgrade Guide* to upgrade NSP.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Once the upgrade is complete and you have access to the NSP UI, follow the steps below.

a. Extract the Installation.zip file received from Nokia and upload the system license to NSP:

b. Open **Centralized License Manager, Network Pool Keys** and click **+ Pool Key**.

c. Choose the file that contains the NSP Routing key (nspRoutingLicense.xml) and click **Upload**.

END OF STEPS

1.6 How do I view license points allocated to each NE?

1.6.1 Purpose

This procedure describes how you can access the license inventory file using the UI. To access the same information using API, see the Network Developer Portal. The license inventory file lists the license points consumed per object per managed NE. Objects are ordered by license product name; the information for each includes the following:

- object FDN, for equipment
- associated site ID, for equipment
- licensed product name
- number of license points that the object consumes

Note: A license file does not include an object that has a licensed quantity of zero.

1.6.2 Steps

1

Open **File Server** from the NSP main menu.

2

In the **Root Directory List**, select **nokia**.

3

Then select **license→inventory→inventory.zip**.

You have to uncompress the file to view the contents of the contained XML file.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.7 What do I need to know about extended NE software support for the NSP license?

1.7.1 Extended NE software support

NSP enables extended NE software support through the NSP license, beginning with N-4 NE release (relative to the NSP release). In order to manage the extended NEs, purchasing extended licenses is recommended.

CLM automatically generates an inventory report showing license points for the nodes and license points consumed. To view the inventory report, open **File Server** and navigate to the **nokia**, **nsp**, **license** folder and uncompress the **extended-support-inventory.zip** file.

To view entitlements for the extended NE software support in the NSP UI, select the **Centralized License Manager**, **Network Pool Keys** view, and expand **NSP Routing**, **Network Element Licenses**.

The supported nodes zip file is automatically installed with NSP. To view this file, open the **Artifacts**, **Artifact Bundles** view. When the zip is uncompressed, the **supported-nodes.xml** file is installed in the File Server.

To view the supported-nodes.xml file, open **File Server** and navigate to **nokia**, **nsp**, **license**, **supported-nodes**, **supported-nodes.xml**. The supported nodes xml file lists the supported nodes with their corresponding supported releases. Any node type and release combination that is not in the supported-node.xml file is considered extended NE support.

The NSP raises alarms if the supported-node file is not found or if it was tampered with. The CLM raises an alarm if consumed entitlements surpass what was licensed. See 1.7.2 “ What does this alarm mean?” (p. 28).

1.7.2 What does this alarm mean?

The view the following alarms, select **Current Alarms** in the main menu.

Alarm	Description
EntitlementResourceAlert	The consumed entitlements exceed the licensed ones.
NSPLicensedComponentNotFound-InCatalogue	There is a mismatch between the inventory.zip file and the license catalog file. Contact Nokia Support for assistance.
NSPSupportedNodesFileNotFound	The NSP bundle fails to install the supported-nodes artifact or if the supported-nodes.xml file is deleted.
NSPSupportedNodesFileTampered	The supported-nodes file has been tampered with or is corrupt.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1.8 How do I receive product and documentation alerts?

1.8.1 Product alerts

You can subscribe to receive the following types of NSP alerts from the Alerts Subscription page of the Nokia Support portal:

- Maintenance
- Security
- LifeCycle
- Informational
- Product Change

You must also regularly check your NFM-P platform vendor websites for information about OS patches, updates, and information about software and hardware issues.

1.8.2 Documentation alerts

You can subscribe to receive NSP documentation alerts for the following from the Documentation Alerts Subscription page of the Nokia Support portal:

- Manuals and Guides
- Release Information
- Technical Notes

1.9 How do I view technical-support alerts?

Note: You must register to view online technical-support information. Contact your Nokia account representative for more information.

1.9.1 Steps

1. Use a browser to open the Nokia Support portal.
2. Click Log in.
3. Enter your user credentials when prompted.
4. Click Products.
5. Specify NSP (Network Services Platform).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The product may be listed as a favorite below the PRODUCT NAME heading.

6

Click Product Alerts.

7

The Alerts for NSP (Network Services Platform) page opens.

8

To view an alert, click on a link in the Alert (PDF) column.

9

To receive an e-mail notification each time an alert is issued, click Subscribe for Alerts. See 1.8.1 “Product alerts” (p. 30) for information.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2 NSP access and UI administration

2.1 What is NSP access administration?

2.1.1 Introduction

This chapter describes NSP UI access requirements and best practices, and includes procedures for configuring global UI settings and client access.

2.1.2 Browser access to redundant NSP clusters

If you open a browser to the primary NSP URL in a DR deployment, the primary NSP sign-in page opens.

If you open a browser to the standby NSP URL, the browser is redirected to the primary NSP URL if the standby server is operational; otherwise, the browser shows the standby URL as unreachable.

Single-address DR NSP system access

To reduce the number of IP addresses that an NSP operator requires for access to the servers in a DR NSP deployment, you can use a reverse-proxy server to set one IP address for NSP access, regardless of which NSP cluster is active.

See 2.2 “How do I enable single-address DR NSP system access?” (p. 35) for proxy-server configuration information.

2.1.3 Best practices for NSP UI access

Some HTTP errors or stalled user sessions can be avoided by adhering to the following best practices:

- The NSP UI is supported on the latest version of Google Chrome. Although other browser types are supported, Chrome is the preferred browser. For information about additional browser support, see the *NSP Planning Guide*.
- It is recommended to use the NSP menu for access to NSP functions, as user-created links to the functions may be broken by an NSP cluster switchover or software upgrade.
- Enable cookies in your browser.
- Before signing in as a different user, close all other NSP tabs and sign out of the last tab.
- If multiple NSP tabs are open in one browser, close all other NSP tabs before signing out of the last NSP tab; do not just close the browser.
- Avoid pausing a polling function for more than ten minutes.
- In the event of an NSP cluster switchover or shutdown, close all browser tabs; you can sign in again when the server returns to service.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2.1.4 OSS API access to NSP functions

NSP functions publish RESTCONF API URLs for access to managed resources and internal NSP services. Each domain documents the available URLs, which are accessible through a browser to clients such as OSS applications.

See the Network Developer Portal for information about OSS access to the NSP using RESTCONF APIs.

2.1.5 User documentation access

You can open the NSP Help Center from each NSP view by clicking on the ? icon. The Help Center provides domain-specific help and access to other NSP documentation.

2.1.6 Session connection loss

NSP UI sessions that are terminated by a connection loss may require up to two minutes to reset after the connection is restored. In the interim, the UI may seem to function, but executing a command results in a browser error. The condition persists until an automated system function clears the former session.

2.1.7 Keyboard-based navigation

You can use the keyboard to navigate and interact with many NSP views. Keyboard navigation allows you to highlight and select interactive elements using keystrokes instead of a pointing device.

The following table lists the accessibility options.

Keystroke	Action
Tab	Advance to next element
Shift + Tab	Return to previous element
Alt + down arrow Option/Alt + down arrow in Apple/OSX	Open pop-up or drop-down menu
Shift + F10 Shift + Fn + F10 in Apple/OSX	Open contextual menu
Ctrl + c Command + c in Apple/OSX	Copy
Ctrl + v Command + v in Apple/OSX	Paste
Enter	Open folder or expandable object such as tile Invoke action on button or menu item
F8 Fn + F8 in Apple/OSX	Move over larger elements or to next page

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Keystroke	Action
F5 Shift + Fn + F5 in Apple/OSX	Refresh
Shift + F1 Shift + Fn + F1 in Apple/OSX	Open tool tip
Esc	Close tool tip or menu
Arrow	After tile in matrix selected using Tab key, navigate among tiles Up and down arrows for navigation through items in open contextual or pop-up menu Up and down arrows for navigation between table rows Left and right arrows for navigation across table column headers
Shift + right or left arrow	Reorder data-table columns in selected header

2.2 How do I enable single-address DR NSP system access?

2.2.1 Purpose

Use this procedure to reduce the number of IP addresses a user requires for access to the NSP clusters in a DR NSP deployment.

The procedure describes implementing a reverse proxy that presents only one IP address for system access. The reverse proxy maps the IP address to the appropriate NSP cluster.

Note: The procedure describes using the mod_proxy Apache HTTP module. Using a different proxy agent or mod_proxy configuration is supported but not described. Also, mod_proxy installation is not described. The reverse proxy must function as an external system; it is not a built-in feature of NSP. Reverse proxy implementation is specific to a network; the network administrator must determine which implementation is best suited to the management network.

2.2.2 Steps

1

Log in as the root user on the station that is to host the reverse proxy.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Open the httpd.conf file in the mod_proxy installation directory using a plain-text editor such as vi.

4

Edit the file to include the following:

```
<VirtualHost *:*>
    <Proxy nspOS://dr>
        BalancerMember http://NSP1
        BalancerMember http://NSP2
    </Proxy>
    ProxyPreserveHost Off
    ProxyPass / nspOS://dr/
    ProxyPassReverse / nspOS://dr/
</VirtualHost>
```

where

NSP1 and *NSP2* are the advertised addresses of the NSP clusters

5

Close the console window.

END OF STEPS

2.3 How do I configure NSP system settings?

2.3.1 Purpose

Use this procedure to specify the default operating parameters for NSP users.

2.3.2 Steps

1

Log in to NSP as an administrator.

2

On the NSP banner bar, click **User**, **Settings**.

3

Click **System Settings** on the navigation panel.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Configure any of the following global parameters:

- Specify the Polling Time interval for information display updates.
- Set the GUI Language preference.
- Set or modify the Security Statement text that appears on the NSP sign-in page. You can also set an option that requires users to acknowledge the security statement before they can login.
- Select or clear the **Row Color With Severity** option to display or hide the alarm severity color in alarm tables.
- Configure the Time Zone parameter, which affects the timestamp of alarm messages.
- To specify a tile server for map operations, configure the Map Settings parameters:
  - Background Map Layer URL: link to a map available under an open license, in the following format:
    https://*tile_server*/*path*/*file*.png
  - Background Map Layer Attribution: optional free-form text field for crediting an open license provider for legal purposes

5

Click **Save** when you have finished changing system settings.

END OF STEPS

2.4 How do I configure alarm-severity colors?

2.4.1 Purpose

Use this procedure to specify the display colors for alarm levels.

2.4.2 Steps

1

Login to NSP as an administrator.

2

On the NSP banner bar, click **User**, **Settings**.

3

Click **Alarm Colors** on the navigation panel.

4

Under Select Alarm Type, select a severity level and then click on a color tile in the Background Color palette to assign a background color to the severity level. The hexadecimal code for the color appears in the text field beside the palette.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Repeat this step to set custom colors for other alarm severity levels.

5

Click **Save** when you have finished changing settings.

END OF STEPS

2.5 How do I customize the main menu?

2.5.1 Purpose

Use this procedure to reorganize or display/hide main menu items.

You can create functional areas and folders to organize menu items, and you can create links to external URLs. Functional areas are used as visual aids that divide menu items into categories. Folders are used similarly, but can be opened and closed to display or hide their contents, thereby managing the size of the main menu.

2.5.2 Steps

1

Login to NSP as an administrator.

2

On the NSP banner bar, click **User**, **Settings**.

3

Click **Customize Main Menu** on the navigation panel.

4

In the Customize Main Menu form, perform any of the actions listed below.

Hide or display a menu item

5

On a menu item click or to hide or display the item.

If you hide or display a functional area or a folder, all of the items within it are hidden or displayed.

Move a menu item

6

Click on a menu item and drag it to a new position on the menu. The ⁝⁝ **Drag** icon indicates that the item is moveable.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If you move a functional area or a folder, all of the items within it are moved.

Create a menu item

7

Newly-created items are added at the bottom of the menu list, from which you can drag them to other locations.

At the bottom of the menu list, click **New**, followed by one of the following:

- **Functional Area:** specify a name for the functional area.
- **Folder:** specify a name for the folder.
- **Link:** specify a URL in the Link field, a name (as it will appear in the menu) in the **Name** field. Descriptive text is optional. If you want the link to open in a new browser tab, enable the **Open In New Tab** option.

8

To remove a functional area, folder, or link, click on the item and click **Delete**. You cannot delete NSP components from the menu.

Revert to default menu settings

9

Click **Restore To Default**.

Note: The Restore To Default command removes *all* menu customizations from *all* sessions (current and past), and restores the NSP main menu to its original design. If you have clicked it in error, click **Discard Changes** immediately.

10

Click **Save** when you have finished changing settings.

END OF STEPS

2.6 How do I configure linked URLs?

2.6.1 Purpose

Use this procedure to link up to 20 external URLs that NSP users can open in a new browser tab from the More menu on the NSP banner.

2.6.2 Steps

1

Login to NSP as an administrator.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

On the NSP banner bar, click **User**, **Settings**.

3

Click **Linked URLs** on the navigation panel.

4

Click **+Add**. The Add Linked URLs form opens.

5

Configure the Name and URL parameters.

6

Click **Add**. The form closes.

7

Click **Save**.

8

To edit a linked URL, click ⋮ **More, Edit**.

9

To remove a linked URL, click ⋮ **More, Delete**.

10

Click **Save** when you have finished changing settings.

END OF STEPS

2.7 How do I configure event logging?

2.7.1 Purpose

Use this procedure to configure the recording of assurance events, or to purge all event records from the database.

Note: Events can be retained for up to 30 days.

2.7.2 Steps

1

Login to NSP as an administrator.

2

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

On the NSP banner bar, click **User**, **Settings**.

3

Click **Event Logging Policy** on the navigation panel.

4

Turn on the **Enable event logging** option.

5

To specify how long event records are retained, configure the Retention Time parameter.

6

Click **Delete Stored Events** to remove preexisting log events.

7

Click **Save** when you have finished changing settings.

END OF STEPS

2.8 How do I configure an e-mail server for notifications?

2.8.1 Purpose

Use this procedure to configure connection information for an e-mail server. The e-mail feature may be used to contact NSP users, send alarm notifications as configured in an alarm policy, or provide notifications of scheduled Analytics reports.

You can configure only one e-mail server in an NSP deployment.

2.8.2 Steps

1

Sign in to the NSP as an administrator.

2

On the NSP banner bar, click **User**, **Settings**.

3

Click **E-mail Server Configuration** on the navigation panel.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Configure the parameters listed in the following table.

Parameters	Notes
E-mail server address	IPv4 address, hostname, or FQDN of e-mail server An e-mail server with an IPv6 address must use a hostname or FQDN. A hostname or FQDN must be DNS resolvable.
Port number	TCP listening port on e-mail server
E-mail address	Sending e-mail address of e-mail notifications
Username and Password	Authentication credentials for e-mail server
Protocol	E-mail authentication protocol The SMTP option is not secure. In order to enable secure e-mail notifications using the SMTPS or STARTTLS option, you must: • Ensure that the mail server TLS certificate is specified in the trustedCertificates parameter in nsp-config.yml: /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml Example: **trustedCertificates: ["/opt/certs/mail.pem", "/opt/certs/*otherCert*.pem", "/opt/certs/*otherCert*.pem"]** Where trustedCertificates specifies a comma-separated list of paths to certificate files. The above example includes the path to the **mail.pem** mail server TLS certificate. • Run config/deploy on the NSP deployer VM to install the mail server certificate on the system: # **/opt/nsp/NSP-CN-DEP-*release-ID*/bin/nspdeployerctl install --config --deploy** ↵

5

The Test and Test Email to Current User functions are highlighted when the e-mail server configuration is updated.

Perform one or more of the following, as required.

a. To send a test message to the specified e-mail server and address, click **Test**.

b. Click **Test Email to Current User** to send a test message to the currently logged in user. Such an action is recommended to verify successful e-mail delivery before turning on the global Verify Email setting in Users and System Security.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Click **Save** when you have finished changing settings.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3 Map layout

3.1 What is the Map Layout?

3.1.1 Introduction

A Map Layout lets administrators specify a common map layout with global location information for NEs and routers, for use in NSP map views.

The Map Layout has two layers: physical and IGP. In the physical map layer, NEs can be grouped into logical groups called regions and zones that are organized against a background map. In the IGP layer, routers are similarly grouped into regions and zones against the same map background. The map can be zoomed out to the regional or continental level, or zoomed in to the city street level, providing precise information about network equipment locations.

The IGP map layer is initially created the first time you select the IGP layer in the Map Layout. It is created based on information derived from the physical layer. Routers in a newly-created IGP layer have corresponding NEs at the same location in the physical layer. Regions and zones in a newly-created IGP layer have corresponding regions and zones at the same location in the physical layer. The regions and zones in the initially-generated IGP layer cannot be deleted and the routers in these regions and zones cannot be excluded. In cases where a router has discovered a subnet, the subnet object is placed in the same region as its designated router. The physical layer must be configured before you can create an IGP layer.

Once the IGP layer is created, you can create additional regions and zones in the IGP layer that do not have corresponding regions and zones in the physical layer. Similarly, you can add routers without corresponding NEs to regions in the IGP layer.

Note: The physical layer of the Map Layout view should be accessed by only a single administrative user at any given time, via a single session within Map Layout. Simultaneous access by multiple users could result in version conflicts and error messages. While working in the Map Layout, if you are unsure if there have been changes to the Map Layout, click Refresh before continuing to make changes.

Note: Deleting the Map Layout will result in the view deletion always displaying as ‘in progress’. As a workaround, refresh the browser, or only delete the IGP Map Layout in the IGP selection and not the Physical selection.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 3-1 Map Layout with regions



Use the controls on the map palette to adjust the behavior and appearance of the map and objects.

When objects share the same physical location, the map shows a multi-layered icon shaded in blue. To see the co-located objects individually, drag them off of the multi-layered icon.

Table 3-1 Map Palette controls

Fit to Screen	Zoom the map to fit the selected region to available screen area.
Clustering controls	Display or hide region and zone boundaries. Option to move all contained objects when moving a region or zone. Display options for connectors to any NEs/routers that are external to a region or zone: • Group external NEs/routers with their immediate parent zone or region; the map displays all connectors to zones or subzones that contain the external NEs. This option shows greater detail. • Group external NEs/routers with their top-level region; the map displays a single connector to the region icon. This option shows less detail.
Adjust vertices	Adjust icon size for NEs/routers, zones, and regions. Show/hide text labels for map objects.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 3-1 Map Palette controls (continued)

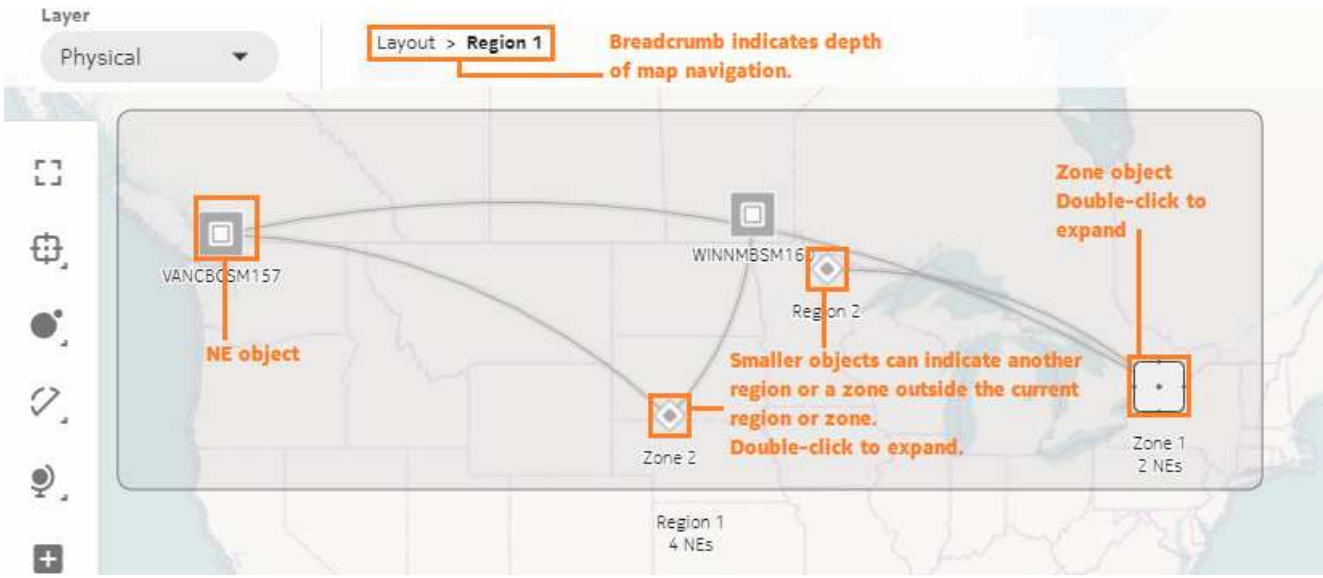
Adjust Links	Show or hide links between NEs/routers, zones, and regions.
Map View	Turn on Bird's-eye View (shows entire map in small inset). Adjust the opacity of the background map.
Zoom	Zoom into and out from the map.

3.1.2 Regions

A region is the basic organizational object of the Map Layout. The layout must contain at least one region, in which NEs/routers are placed. Typically, a region would represent an organizational area of network equipment. Double-clicking a region on the Map Layout displays its contained NEs/routers and nested zones. Double-clicking a nested zone within a region displays its contained NEs/routers and further-nested zones. Right-clicking a region object and choosing the **Back To** menu option takes you up one level in the map hierarchy.

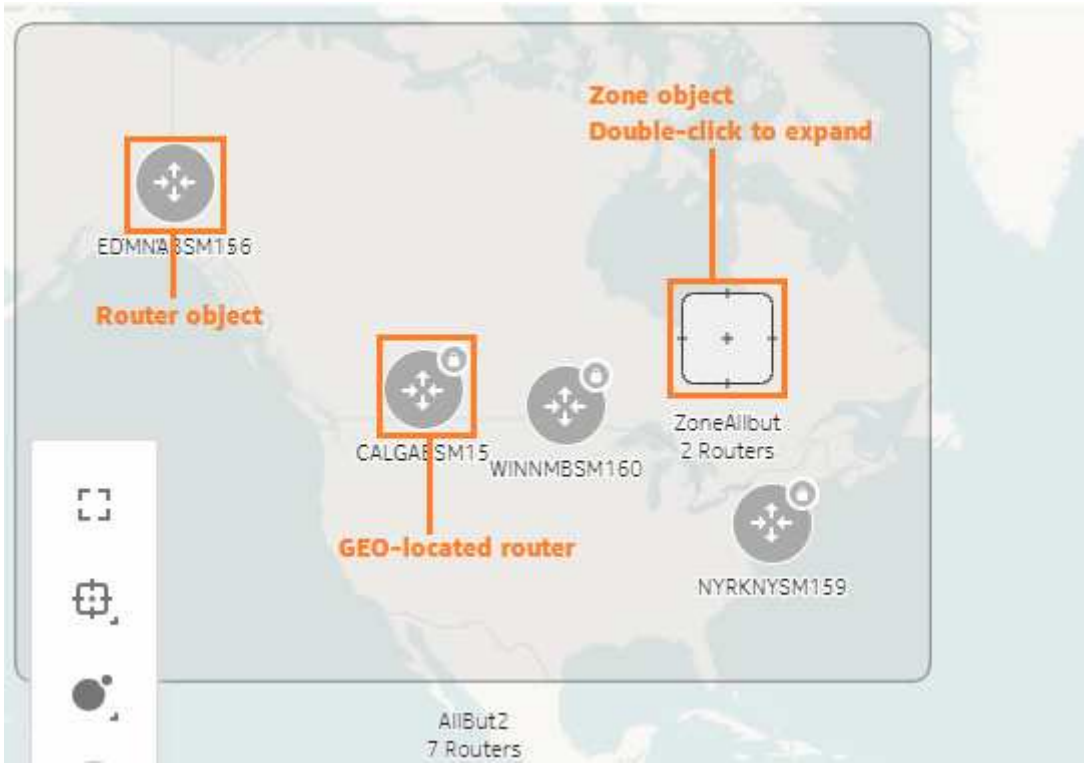
NEs and routers must be assigned to a region to appear on the Map Layout. NEs and routers that are not assigned to a region can be manually assigned to one. NEs are typically included in regions by way of inclusion filters. Newly-discovered NEs are automatically added to a region, provided the region is configured with inclusion filters, and the NEs match the filter criteria. If the Map Layout has GEO positioning enabled, newly-discovered NEs are positioned in a region according to the NE's location information, otherwise newly-discovered NEs are placed in a default position in the region.

Figure 3-2 Exploring region contents - physical layer



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 3-3 Exploring region contents - IGP layer



Right-click on a region to do the following:

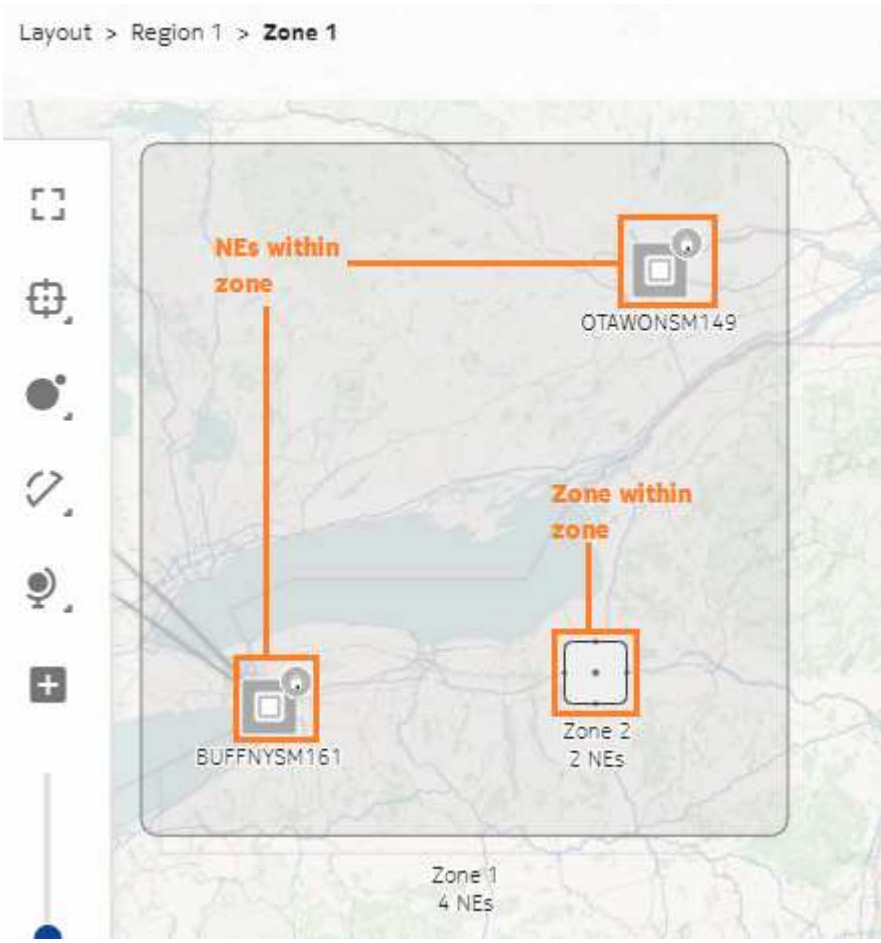
- **Open** expands the region to display its NEs/routers and zones
- **Review** open the region in a configuration form in which you can view the contents of the region
- **Edit** open the region in a configuration form in which you can add or remove NEs/routers from the region
- **Delete** removes the region from the Map Layout, along with all contained NEs/routers and zones

Zones

A region may contain more NEs/routers than can manageably fit on the Map Layout; for example, in a densely-populated area. You can organize the Map Layout by sub-grouping the NEs/routers into zones. You can add zones to a region and you can add zones within zones. Double-clicking a zone displays its contained NEs/routers and nested zones. Right-clicking a zone object and choosing the **Back To** menu option takes you up one level in the map hierarchy.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 3-4 Exploring zone contents - physical layer



Right-click on a zone to do the following:

- **Open** expands the zone to display its NEs/routers and zones
- **Rename** opens a configuration form in which you can change the zone name
- **Cut** removes the zone from the map and places it on the clipboard. Right-click at another location and choose **Paste** to place the zone.
- **Delete** removes the zone from the Map Layout, and places all contained NEs/routers in the current Zone or Region

3.1.3 Import regions and zones from NFM-P

You can choose an option to import NFM-P equipment groups to automatically create regions and zones. Equipment group hierarchies and layout information are imported from NFM-P and converted into regions on the Map Layout. Any nested equipment groups from NFM-P become zones in the Map Layout.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.1.4 Import NE location information from NFM-P

You can choose an option to import your NEs' stored GEO location information. Information from either the Coordinates field or the Latitude/Longitude In Degrees fields is used to establish the geographical location of imported NEs.

The following examples reflect the types of supported latitude/longitude string formats:

- N 45 58 23, W 34 56 12
- N37 37' 00 latitude, W122 22' 00 longitude
- N36*39.246' W121*40.121'

You can enable GEO positioning for the Map Layout after it is created; see 3.13 "How do I enable GEO positioning for NEs and routers?" (p. 59).

3.2 Pathway: create and configure a physical Map Layout

3.2.1 Steps

1

(Optional) Specify a Background Map Layer URL in the NSP system settings; see 2.3 "How do I configure NSP system settings?" (p. 36).

2

Create a physical layout; see 3.4 "How do I create a physical Map Layout?" (p. 51).

You can import NFM-P equipment groups to automatically create map regions or zones as part of this step, or you can create an empty layout and add regions one at a time.

3

(Optional) Add regions to the layout; see 3.6 "How do I create a region for a physical Map Layout?" (p. 53).

4

(Optional) Position regions on the map view; see 3.8 "How do I place a region on the Map Layout?" (p. 55).

5

(Optional) Create zones to organize NEs within regions; see 3.9 "How do I create a zone in the Map Layout?" (p. 56).

END OF STEPS

3.3 Pathway: create and configure an IGP Map Layout

Note: The physical Map Layout layer must be configured before you can create an IGP layer.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.3.1 Steps

1

Create an IGP layout; see 3.5 “How do I create an IGP Map Layout?” (p. 52).

2

(Optional) Add regions to the layout; see 3.7 “How do I create a region for an IGP Map Layout?” (p. 54).

3

(Optional) Position regions on the map view; see 3.8 “How do I place a region on the Map Layout?” (p. 55).

4

(Optional) Create zones to organize routers within regions; see 3.9 “How do I create a zone in the Map Layout?” (p. 56).

END OF STEPS

3.4 How do I create a physical Map Layout?

3.4.1 Purpose

Complete this procedure to create a common physical map layout for NSP map views. You can only create one layout.

You can create your Map Layout with regions and zones, based on imported NFM-P equipment groups, or you can create an empty layout and add regions one at a time.

Note: The physical Map Layout GUI must be allowed to complete before the user attempts to open another browser tab or start other Map Layout actions. Wait until the progress indicator indicates the Map Layout creation is complete before performing other actions to avoid this problem.

3.4.2 Steps

1

Open Map Layout.

2

If no Map Layout is configured in the NSP, a No Map Layout Created message appears in the GUI. Click **Add New Layout**.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

In the Add New Layout form, specify a **Layout Name** and select an option to position or import NEs:

- **NE Positioning - Geographic Coordinate System:** NE objects are positioned on the Map Layout based on the NEs' geographical coordinates. NE coordinate information may be stored in the NFM-P database, or directly on individual NEs.
- **NE Positioning - Cartesian Coordinate System:** NE objects are positioned on the Map Layout based on the NEs' cartesian coordinates. NE coordinate information may be stored in the NFM-P database, or directly on individual NEs.
- **Import NFM-P Top Level Equipment Groups Into Regions:** each top level equipment group from NFM-P is created as a region in NSP, with sub-groups created as zones within the regions.

  If you want to automatically organize NEs into regions or zones, based on equipment groups imported from NFM-P, enable the **Automatically Create Regions** option and enable one of the import options:
- **Import NFM-P Top Level Equipment Groups Into Zones:** a single region is created in NSP, with each top level equipment group from NFM-P created as a zone within the region. This option is intended for smaller networks where only one region is needed.

  Each NFM-P equipment group is imported and converted to a region or zone. NFM-P map coordinates are also imported.

4

Click **Ok**.

5

The new layout is added to the Map Layout GUI in the Physical layer.

Complete 3.6 "How do I create a region for a physical Map Layout?" (p. 53) to create and add more regions to the layout.

END OF STEPS

3.5 How do I create an IGP Map Layout?

3.5.1 Purpose

Complete this procedure to add an IGP layer to the Map Layout for NSP map views. The IGP map is created with information from regions, zones, and NEs in the physical Map Layout. The resulting IGP map layer is populated with corresponding regions, zones, and routers. You must have a physical map configured before you can create an IGP map; see 3.4 "How do I create a physical Map Layout?" (p. 51).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.5.2 Steps

1

Open Map Layout.

2

Select IGP from the **Layer** drop-down list.

3

You are prompted to generate an IGP layer. Click **Ok**.

4

The IGP layer is generated. This process may take several minutes.

Complete 3.7 “How do I create a region for an IGP Map Layout?” (p. 54) to add more regions to the layout.

End of steps

3.6 How do I create a region for a physical Map Layout?

3.6.1 Purpose

Complete this procedure to add regions to a physical Map Layout. You can create multiple regions.

When you configure a region, you can configure inclusion filters that automatically associate NEs with the region, based on filter criteria. Newly-discovered NEs are automatically added to a region, provided they match the region’s filters. If the region is not configured with inclusion filters, it is static and unchanging.

3.6.2 Steps

1

Open Map Layout.

2

In the Map Layout GUI, select **Physical** from the **Layer** drop-down list.

3

Click ＋**Add Region**.

4

In the Create Region form, specify a name and description for the region.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Specify NEs for the region, either manually or through inclusion filters:

- **Add NEs to the region manually.** Select **Manual Entry** from the drop-down list. Then click **Import** to import a comma-separated list of NE management IP addresses.
- **Filter NEs based on advanced filter expressions.** Select **Advanced Filter** from the drop-down list. Then click **Filter**.

  In the Advanced Filter form, type a filter expression in the **Filter Expression** field, starting with an NE attribute, followed by a Boolean operator and an attribute value. The system suggests possible attributes, operators, and attribute values as you type, and displays error messages in red when an expression is invalid. You can combine attribute-value expressions using AND and OR operators.

  You can also use the Expression Builder; select a **Filter Attribute**, followed by a **Filter Operator**, and a **Filter Value**. Then click **+Add**. The expression is added to the **Filter Expression** field.

  Any IPv6 addresses in an advanced filter expression must be enclosed in single quotation marks (‘ ‘).

  When you have finished configuring your filter expressions, click **Apply Filter**.

Note: If you are creating a filter to include a large number of NEs, it is better to specify an attribute with a range of values to include the NEs. Specifying a large number of individual NE attribute values linked together with OR operators creates a complex inclusion filter that will burden system resources and possibly cause the import process to fail.
Any IPv6 addresses in an advanced filter expression must be enclosed in single quotation marks (‘ ‘).

The imported NEs or filter-included NEs are listed in the Create Region form.

6

Review the list of NEs to include in the region. Click **Submit** to save the region.

END OF STEPS

3.7 How do I create a region for an IGP Map Layout?

3.7.1 Purpose

Complete this procedure to add regions to the IGP Map Layout. You can create multiple regions.

3.7.2 Steps

1

Open Map Layout.

2

In the Map Layout view, select **IGP** from the **Layer** drop-down list.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Click ＋**Add Region**.

4

In the Add Region form, specify a name and description for the region.

5

Specify Routers for the region, either manually or through inclusion filters:

- **Add Routers to the region manually.** Select **Manual Entry** from the drop-down list. Then click **Import** to import a comma-separated list of Router IDs.
- **Filter Routers based on advanced filter expressions.** Select **Filter Expression** from the drop-down list. Then click **Filter**.

  In the Advanced Filter form, type a filter expression in the **Filter Expression** field, starting with a Router attribute, followed by a Boolean operator and an attribute value. The system suggests possible attributes, operators, and attribute values as you type, and displays error messages in red when an expression is invalid. You can combine attribute-value expressions using AND and OR operators.

  You can also use the Expression Builder; select a **Filter Attribute**, followed by a **Filter Operator**, and a **Filter Value**. Then click **+Add**. The expression is added to the **Filter Expression** field.

Note: If you are creating a filter to include a large number of routers, it is better to specify an attribute with a range of values to include the routers. Specifying a large number of individual router attribute values linked together with OR operators creates a complex inclusion filter that will burden system resources and possibly cause the import process to fail.
Any IPv6 addresses in an advanced filter expression must be enclosed in single quotation marks (‘ ‘).

The imported routers or filter-included routers are listed in the Create Region form.

6

Review the list of Routers to include in the region. Click **Finish** to save the region.

End of steps

3.8 How do I place a region on the Map Layout?

3.8.1 Purpose

If a newly-created region is GEO located and contains at least one GEO-located NE or router, the region is placed automatically on the Map Layout. If the region is not GEO-located, it must be manually placed and sized on the map.

Note: If no background map graphic appears in the Map Layout GUI, it can be configured through the NSP system settings; see 2.3 “How do I configure NSP system settings?” (p. 36).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.8.2 Steps

1

Open Map Layout.

2

In the Map Layout GUI, select Physical or IGP from the **Layer** drop-down list, depending on which map layer you want to add a region to.

3

Click **Unplaced Regions**.

A red flag on the icon indicates that unplaced regions are present. Newly-created regions may take up to 30 seconds to become completely available in the Map Layout GUI.

4

In the **Unplaced Regions** list, click on a region icon to place it on the map. On the map, click and drag the region into position.

The Move Zone/Region With Contents option must be enabled on the map palette under **Clustering Controls** before you can add a region to the map.

5

Double-click the region to expand it and move NE or router icons into position.

6

Click **Deploy Layout Changes To Common Layout** to save your changes.

END OF STEPS

3.9 How do I create a zone in the Map Layout?

Note: You can create a zone within a region, or within another zone.

3.9.1 Steps

1

Open Map Layout.

2

In the Map Layout GUI, select Physical or IGP from the **Layer** drop-down list, depending on which map layer you want to add a zone to.

3

Double-click a region on the map. The region expands.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Complete Step 5 or Step 6 as needed.

5

To add a zone to the region, do the following:

a. Click **+Add Zone** on the right-hand side of the GUI.

b. pecify a name for the zone and click **Ok**. The zone is placed in the region.

Zone In the Add New Zone form, snames must be unique across the Map Layout.

c. Click and drag the zone into position on the map.

6

To add a zone to a zone, do the following:

a. Double-click on the zone you want to add a zone to. The zone expands.

b. Click **+Add Zone** on the right-hand side of the GUI.

c. In the Add New Zone form, specify a name for the zone and click **Ok**. The zone is placed in the parent zone.

Zone names must be unique across the Map Layout.

d. Click and drag the zone into position on the map.

7

Click **Deploy Layout Changes To Common Layout** to save your changes.

END OF STEPS

3.10 How do I associate NEs or routers with a region?

3.10.1 Purpose

Use this procedure to search for NEs or routers and manually associate them with a region in the Map Layout.

NEs can also be included in a region by way of inclusion filters. If you configure a region's inclusion filter criteria to match a newly-discovered NE, then the NE is automatically added to a region; see 3.6 "How do I create a region for a physical Map Layout?" (p. 53).

Note: Nokia recommends that each NE/router be associated with only one region.

3.10.2 Steps

1

Open Map Layout.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

In the Map Layout GUI, select Physical or IGP from the **Layer** drop-down list, depending on which map layer you need to work in.

3

Click **NEs Without a Region** or **Routers Without a Region**.

A red flag on the icon indicates that NEs or routers with no region are present.

4

The NEs|Routers Without a Region form opens with a list of all objects not associated with a region.

Do one of the following to associate an NE/router with a region:

- Search the list and click on an object you want to associate with a region. Click **Associate**. A list of available regions is displayed. Click on the region you want to add the object to and click **Associate** to add it to the region.
- Click **Add Filter** and type the name of the region you want to add NEs/routers to. The list contents reduce to show only objects not associated with the specified region.

  Click on an object in the list and click **Associate** to add it to the region.

5

Click **Close**.

6

After you have associated NEs or routers with a region, you must place those objects on the map.

1. Expand the region(s) you associated NEs/routers to.

   Newly-associated NEs/routers may take up to 30 seconds to become completely available in the Map Layout GU.
2. Drag NEs/routers into position and click **Deploy Layout Changes To Common Layout** to save your changes.

If you do not place an NE or router after associating it with a region, it is assigned a default location in the region.

END OF STEPS

3.11 How do I add NEs to a zone?

3.11.1 Purpose

Use this procedure to move NE objects on the Map Layout into a zone, or to any location on the map.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.11.2 Steps

1

Open Map Layout.

2

Select NE objects singly by clicking them on the map. Select multiple NEs by pressing Ctrl+Click and dragging over the objects. Select additional objects by pressing Ctrl+Click.

Press Alt+Click to select a GEO located ( ) NE. You can only move one GEO located NE at a time.

3

Right-click the selected NEs and select the Cut menu command.

4

Right-click the zone where you want to move the NEs and select the Paste menu command.

5

When prompted, click Deploy to save your Map Layout changes.

END OF STEPS

3.12 How do I move connector objects in the Map Layout?

3.12.1 Select and drag

You can select connector objects by clicking them. Move the selected object by dragging it on the map.

When you move a connector from a lower level of the map (i.e., from within a region or zone), the position of the connector is not saved.

3.13 How do I enable GEO positioning for NEs and routers?

3.13.1 Purpose

You can enable an option on the Map Layout to move all NE and router objects into positions on the map, based on each object's stored system coordinates information (latitude/longitude).

GEO positioned NEs and routers appear with Lock badges on the icons. You must press Alt+Click to select and move GEO positioned objects. Regions containing GEO positioned objects are also flagged.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

System coordinates string format

NE and router system coordinates information must be formatted in such a way that NSP recognizes it. The coordinates are configured as GPS latitude and longitude information, in a pair of four-dimensional vectors:

<*direction hours minutes seconds*>, <*direction hours minutes seconds*>

where *direction* is one of the four basic values: N, S, E, W, *hours* ranges from 0 to 180 (for latitude) and 0 to 90 for longitude, and *minutes* and *seconds* ranges from 0 to 60. W 122 56 89 is an example of longitude and N 85 66 43 is an example of latitude.

NSP recognizes system coordinates in the following formats:

- N 45 58 23, W 34 56 12
- N45 58' 23 latitude, W34 56' 12 longitude
- N45*58.23' W34*56.12'
- Decimal Degrees (DD) coordinates are supported in the following formats:
  - '-48.3537, -11.7750',
  - '(48.3537, -11.7750)'
  - (48.3537, -11.7750)
  - ('-48.3537, -11.7750')

  For signed notation (+/-), the range for Latitude is -180 to +180, and for Longitude is -90 to +90.

3.13.2 Steps

1

Open Map Layout.

2

Click ···**More**, **Layout**, **Edit**.

3

In the Edit Layout form, enable either the **NE Positioning, Geographic Coordinate System** or **NE Positioning, Cartesian Coordinate System** option and click **Update**.

Objects are positioned on the map according to their stored location data.

END OF STEPS

3.14 How do I rename the Map Layout?

3.14.1 Purpose

You can rename the Map Layout after it has been configured.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.14.2 Steps

1

Open Map Layout.

2

Click ···**More**, **Layout**, **Edit**.

3

In the Edit Layout form, type a new Layout Name and click **Update**.

END OF STEPS

3.15 How do I move an object to a specific GEO location?

3.15.1 Purpose

You can specify a precise map location information for an individual NE, router, or zone object. You can also restore an object's location to its original location, based on information retrieved from the NSP database.

This function applies only if the Map Layout has GEO information enabled.

3.15.2 Steps

1

Open Map Layout.

2

Right-click an object on the map and select **Move To** from the menu.

3

Specify **Latitude** and **Longitude** coordinates for the object and click **OK**.

To move an object back to its original location, right-click the object and select **Restore to NE | Router | Zone GEO Location** from the menu.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.16 How do I search for objects in the Map Layout?

3.16.1 Purpose

Use this procedure to search for an NE, router, region, or zone on the Map Layout.

Note: If using an IPv6 management IP address as filter criteria in the Map Layout GUI when manually defining the contents of a supervision group, the IP address must be a full exact match of the NE or port. Otherwise, the group will be empty. To work around this issue, use the auto-create groups feature, or when using manually defined filters, use parameters other than IPv6 management IP addresses.

3.16.2 Steps

1

Open Map Layout.

2

In the Map Layout GUI, select Physical or IGP from the **Layer** drop-down list, depending on which map layer you need to work in.

3

Click **Find in Map**.

4

Select any of the available object types from the menu. For example:

- Region name
- Zone name
- NE - by name, management IP, or system ID
- Router - by name or router ID

5

Type a search string in the text field. The list populates with near matches as you type.

The list displays a maximum of 50 results. If the item you are trying to find is not in the list, refine your search string to reduce the number of possible matches.

6

Click on an entry in the list to go to the object's location in the Map Layout.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3.17 How do I cancel un-deployed changes to the Map Layout?

3.17.1 Purpose

Use this procedure to cancel changes you have made to the Map Layout that have not yet been deployed.

3.17.2 Steps

1

Click the **Refresh** button and then click **Continue**.

END OF STEPS

3.18 What are best practices when using the Map Layout?

3.18.1 Best practices

Nokia recommends the following practices when configuring the Map Layout.

3.18.2 Editing the Map Layout

The Map Layout function is best accessed by only a single administrative user at a time, via a single instance of the Map Layout. Simultaneous access by multiple users can result in version conflicts and error messages.

While working in the Map Layout, if you are unsure if there have been changes to the Map Layout, click **Refresh** before continuing to make changes.

3.18.3 Each NE in one region only

Nokia recommends that each NE in the Map Layout be associated with only one region. Placing the same NE in multiple regions can result in inaccurate NE counts in the Unplaced Regions list. Also, duplicate NEs will share the same physical location on the map, regardless of which region they are in.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4 Resource pool management

4.1 How are resource pools used with programmable functions?

4.1.1 Resource pool usage

Resource pools are sets of alphanumeric strings that are used with programmable NSP functions, such as network intents. NSP maintains a list of available resource pools and allows administrators to create and modify pools. Resource pools provide a quick, reusable method to assign IP addresses, numbers, or text strings to ports when you are setting up automated processes.

Note: Resource pools have no relationship with network resource groups. The two have completely different functions in NSP.

You can create and manage the following types of resource pools:

- IP Address
- Numerical
- Text String
- Route Distinguisher or Route Target

You can assign utilization alarm thresholds to resource pools so that Warning, Minor, and Major alarms are generated when resource pool utilization exceeds a prescribed threshold. You assign utilization alarm thresholds to resource pools through threshold policies.

4.1.2 Dashboard view

The Dashboard is the default view of the Resource Management GUI. It displays your resource pools as dashlets. You can select which type of pools are displayed from the drop-down menu. The number of pools displayed in the Dashboard can be controlled by filtering the view based on pool name, scope, description, and threshold policy.

4.2 How do I search for a resource pool?

4.2.1 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

In the Dashboard view, select the type of resource pool you are searching from the drop-down list String Pools.

4

Type a search string in the text field. As you type your string, matching pool objects appear in the dashboard.

5

By default, four searchable pool attributes are enabled. Your search string matches pool objects against any of those attributes.

To narrow the scope of your search, click **Remove Attribute** on attributes you don't want to search under.

To add a searchable attribute, click **Add Filter** and select an attribute from the menu.

6

If you enable the **Equals** option, the search only returns pool objects with attribute strings that *exactly match* your search string. If the option is disabled, the search returns pool objects that contain your search string as *part of* an attribute string.

The selection of resource pool dashlets in the dashboard is updated dynamically as you specify a search string, and as you specify filter attributes.

END OF STEPS

4.3 How do I view summary information for a resource pool?

4.3.1 Steps

1

You examine configuration and utilization details for a resource pool in the Pool Summary view. Open a pool in one of the following ways, depending on the view you are working in.

- In the Dashboard view, hover over a resource pool object and click **View**.
- In a resource pool list view, click **More**, **View Pool** on a list item.

2

The resource pool opens in the Pool Summary view, which displays read-only configuration and utilization data for a resource pool. It also lists reserved resources in the pool.

- **Reserve a resource:** Click **Reserve Resource**; see 4.11 "How do I reserve resources?" (p. 73) for information.
- **Modify the resource pool:** Click **Edit Pool** and change the pool configuration as needed.

3

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Click the **Resource Management** breadcrumb to return to the resource pools list.

END OF STEPS

4.4 How do I configure an IP address pool?

4.4.1 Purpose

An IP address pool defines a range of IP addresses that can be applied to specific configurations in NSP programmable functions. The range is defined by an IP mask and an allocation mask.

To support IPv4 subnet repurposing, subnets can be configured with one or more purpose tags.

4.4.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select the **IP Pools** view from the drop-down list.

4

Do one of the following:

- **Create a new pool:** Click ＋**Add Pool**.
- **Modify an existing pool:** In the pool list, click ⋮ **Table Row Actions**, **Update Pool** on a list item.

5

In the Create | Edit IP Pool form, configure the parameters as required.

6

Click ＋**Add** on the IPv4 Networks and Masks list or select a list item and click **Table Row Actions**, **Edit**.

1. Type an IPv4 network/mask length pair in the **IPv4 Mask** field. Use the format ***<ip_address>/<bit_length>***.
2. Type a purpose string in the **Purpose** field and click ＋**Add**. The purpose string is added to the network/mask pair. You can specify additional purpose strings to support IPv4 subnet re-purposing.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3. Click **Add | Update**.

   You are returned to the Create | Edit IP Pool form.

7

To assign a threshold policy to the pool, click in the **Threshold Policy** field and select a policy from the Select Threshold Policy form.

8

Click **Create** or **Update** to save your changes.

End of steps

4.5 Why use IPv4 subnet re-purposing?

4.5.1 Manage address depletion

The networking industry is facing the depletion of un-allocated IPv4 address space. To enable service providers to grow in business, techniques have been introduced to use IPv4 address space more efficiently. While dynamic IP allocation mechanisms like DHCP make it easy to assign new IPv4 addresses to endpoints, it is an operational challenge to update static addresses because all endpoints in the corresponding subnet must be updated accordingly.

The major challenge with traditional resource management is that pools are typically used for one purpose only. Providers would have pools of IPv4 addresses, specific for subscriber host addresses, business services, in-band management, control-plane loopback addresses, transfer networks, management systems, gateway addresses, etc. If operators implement a strategy like using /31 instead of /30 for network interfaces, the freed address space can be used for other purposes. However, only complete address blocks can be taken from one pool and added to another pool.

Under the principle of multi-purpose pools, operators do not need to define dedicated pools for single purposes. Especially for public IPv4 addresses, a single IPv4 pool is sufficient. Every address block inside the pool has purpose tags assigned so that the operator can decide the purpose for each address block. If demand changes over time, the purpose tags can be updated. When address blocks can be assigned multiple purpose tags, they can be used more universally. In addition, purpose tags are only used for new allocations: the user can update the address block purpose without affecting existing reservations or allocations. If all purpose tags are removed from an address block, no new reservations are allocated, providing an efficient method to drain an address block.

4.6 How do I configure a string pool?

4.6.1 Purpose

A String pool defines a template for alpha-numeric values, with a defined syntax, length, and maximum capacity. String pools are applied to specific configurations in NSP programmable functions.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

In the event that a string pool reaches maximum utilization, you can modify the string length and maximum capacity of the pool to increase its size.

4.6.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select the **String Pools** view from the drop-down list.

4

Do one of the following:

- **Create a new pool:** Click ＋**Add Pool**.
- **Modify an existing pool:** In the pool list, click ⋮ **Table Row Actions**, **Update Pool** on a list item.

5

In the Create | Update String Pool form, configure the parameters as required.

Specify the **Pattern** as a regular expression. **String Length** and **Max Capacity** must be integers.

6

To assign a threshold policy to the pool, click in the **Threshold Policy** field and select a policy from the Select Threshold Policy form.

7

Click **Create** or **Update** to save your changes.

END OF STEPS

4.7 How do I configure an RD-RT pool?

4.7.1 Purpose

A Route Distinguisher-Route Target (RD-RT) pool defines a range of numerical values that can be applied to specific configurations in NSP programmable functions.

In the event that an RD-RT pool reaches maximum utilization, you can decrease the minimum value

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

and/or increase the maxim value of the pool to increase the pool size.

4.7.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select the **RD-RT Pools** view from the drop-down list.

4

Do one of the following:

- **Create a new pool:** Click ＋**Add Pool**.
- **Modify an existing pool:** In the pool list, click ⋮ **Table Row Actions**, **Update Pool** on a list item.

5

In the Create | Edit RD-RT Pool form, configure the parameters as required.

Minimum Value and **Maximum Value** must be integers.

6

To assign a threshold policy to the pool, click in the **Threshold Policy** field and select a policy from the Select Threshold Policy form.

7

Click **Crate** or **Update** to save your changes.

END OF STEPS

4.8 How do I configure a Numeric pool?

4.8.1 Purpose

A Numeric pool defines a range of numerical values that can be applied to specific configurations in NSP programmable functions.

In the event that a numeric pool reaches maximum utilization, you can decrease the minimum value and/or increase the maxim value of the pool to increase the pool size.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.8.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select the **Numeric Pools** view from the drop-down list.

4

Do one of the following:

- **Create a new pool:** Click ＋**Add Pool**.
- **Modify an existing pool:** In the pool list, click ⋮ **Table Row Actions**, **Update Pool** on a list item.

5

In the Create | Edit Numeric Pool form, configure the parameters as required.

Minimum Value and **Maximum Value** must be integers.

6

To assign a threshold policy to the pool, click in the **Threshold Policy** field and select a policy from the Select Threshold Policy form.

7

Click **Create** or **Update** to save your changes.

END OF STEPS

4.9 What are threshold policies?

4.9.1 Threshold policies

Threshold policies define a set of numerical thresholds that are used to generate utilization alarms for resource pools. Depending on their intended usage, threshold policies can be configured to define Warning, Minor, and Major alarm thresholds as percentages or integer counts. When you configure a resource pool, you can associate it with a threshold policy.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.10 How do I configure a threshold policy?

4.10.1 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select the **Threshold Policies** view from the drop-down list.

4

Do one of the following:

- **Create a new policy:** Click ＋**CREATE THRESHOLD POLICY**.
- **Modify an existing policy:** In the policy list, click ⋮ **Table Row Actions**, **Edit Threshold Policy** on a list item.

5

In the Create | Edit Threshold Policy form, configure the parameters as required.

6

Select a **Threshold Type** from the drop-down list.

7

Configure **Warning**, **Minor**, and **Major** threshold values.

For a Utilization % threshold policy, the threshold values must be percentages, ascending from the Warning to Major levels.

For a Free Count threshold policy, the threshold values must be integers, ascending from the Warning to Major levels.

8

Click **CREATE** or **UPDATE** to save your changes.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.11 How do I reserve resources?

4.11.1 Purpose

You reserve pool a resource to allocate it for a specific task. You reserve a resource from a resource pool in the Pool Summary view.

4.11.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select a resource pool type from the drop-down list at the top of the GUI.

4

In the pools list, double-click the resource pool from which you want to reserve a resource.

The Pool Summary view opens.

5

Click ＋**Reserve Resource**.

6

In the Reserve Resource form, specify the resource **Reference** and **Owner** in their respective fields.

7

Enable the **Confirmed** option to indicate that the resources are allocated and in use.

If the Confirmed option is not enabled, the resources are reserved with the implication that they will be in use.

8

Specify the resource values you are reserving in the **Reserve Values** field.

You can specify multiple resource values. After typing a value, click ＋**Add** to add it to the list.

9

Enable the **All Or Nothing** option if you want the resource reservation to go ahead only if all of the specified resources are available to be reserved.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If the All Or Nothing option is disabled, the system reserves only the resources that are available.

10

Click **Submit** to reserve the resources.

END OF STEPS

4.12 How do I release a resource?

4.12.1 Purpose

You release a resource back to a resource pool in the Pool Summary view, based on values in its **Reference** or **Owner** fields.

4.12.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select a resource pool type from the drop-down list at the top of the GUI.

4

In the pools list, double-click the resource pool from which you want to release a resource.

The Pool Summary view opens.

5

Click ⋮ **More**, **Release By Reference** or **Release By Owner**.

6

Specify a **Reference** or **Owner** string value, as required.

7

Click **Submit**.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4.13 How do I commit a resource?

4.13.1 Purpose

Use the Commit Resource command to allocate all available pool resources as a batch, where you need a number of resources but do not need to specify precisely which ones. The Commit Resource command returns resources from whatever is available in the pool. The Commit Resource command is available for Numeric, IP Address, and RD-RT pools.

You commit resources from a resource pool in the Pool Summary view.

4.13.2 Steps

1

Open Network Intents.

2

In the upper right-hand corner of the Network Intents GUI, click ⋮ **More**, **Open Resource Management**.

The Resource Management GUI opens in a separate browser tab.

3

Select a resource pool type from the drop-down list at the top of the GUI.

4

In the pools list, double-click the resource pool from which you want to commit resources.

The Pool Summary view opens.

5

On the resource pool list item, click ⋮ **Table Row Actions**, **Commit Resource**.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5 NSP File Server

5.1 What is the NSP File Server?

5.1.1 Overview

The NSP File Server is a file import and management utility that facilitates NSP artifact management for NSP functions such as Device Management, Workflows, and Network Intents.

The NSP File Server.

- facilitates file management for NSP functions
- allows you to:
  - navigate between folders and list files
  - create and remove folders
  - import and remove files
  - search for directories and files by name
  - export a directory listing to a file

Typical uses for the File Server include:

- organizing software images for NE upgrades
- managing input for mass operations such as migrations
- NE backup storage
- managing files used for ZTP
- debug and troubleshooting file storage

5.2 File purge policies

5.2.1 Introduction

To prevent excessive disk consumption, you can configure purge policies that define the file retention criteria.

The purge function has the following configurable policies:

- global policy of default parameters; applies to all File Server directories except directories in the global Ignore List and override policies
- one or more override policies for directories that require purge settings that differ from the global settings; the override policy settings for a directory take precedence over the global settings

The settings are configurable in the NSP File Server UI, as described in 5.4 “How do I configure file purge policies?” (p. 82).

The settings are also configurable using an NSP RESTCONF API; see the Network Developer Portal for information.

Consider the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- An NSP administrator can:
  - view or modify the global purge policy.
  - view, edit, disable, or delete an override policy
- The global policy is always enabled, and cannot be disabled or deleted.
- Files are purged first based on the retention time and then by the disk space usage threshold. If disk usage remains above the critical threshold, a specified cleanup percentage of the oldest files are purged.

5.2.2 Ignore Lists

In each policy type, you can specify an exclusion list of directories called an Ignore List. The directories in an Ignore List are unaffected by the settings in the associated policy.

Special global Ignore List consideration

The global Ignore List includes the following default directories, which must not be removed from the list:

- /lsom/neSoftware
- /lsom/neUpgrade
- /nokia/nsp/faultManagement/sounds
- /nokia/nsp/cam
- /nokia/nsp/i18n
- /nokia/nsp/mdm
- /ztp
- internal

If you accidentally remove a default directory from the global Ignore List, you must return the directory to the list before you complete your configuration activity.

Also, if you use the RESTCONF API to add a directory to an Ignore List, you must include all current directories in the list, and append any new directories to the list, for example:

```
"ignoreFileList": "/lsom/neSoftware,/lsom/neUpgrade,/nokia/nsp/cam,
/nokia/nsp/faultManagement/sounds,/nokia/nsp/i18n,/nokia/nsp/mdm,
/ztp,internal,new_directory_1,new_directory_2"
```

5.3 How do I use the NSP File Server?

5.3.1 Purpose

Perform this procedure to perform file-management functions using the NSP File Server.

Note: The NSP File Server supports the typical multi-select functions using the Shift and CTRL keys.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5.3.2 Steps

1

From the **NSP Menu**, select **File Server**.

The left pane displays the Directory List; the content pane, which is adjacent, lists the objects in the selected directory, and the collapsible Info pane at the right side displays information about the currently selected file or directory.

Basic navigation

2

To scroll through a list of directories or files, use either of the following:

- the scroll bar
- the Page Up and Page Down keys
- the up and down cursor keys.

3

To display the content of a directory in the Directory List, click on the directory.

The directory contents are displayed in the content pane.

The content panel has all the records in the directory. The total number of records are displayed at the bottom of the pane.

4

To open a directory in the content pane, double-click on the directory, or click ⋮ beside the directory and click **Open Directory**.

5

To collapse or expand the Info pane, click > or < at the right content pane border.

Display operations

6

To filter the list of objects in the content pane, click ▽ below a column heading and specify the search criteria using Boolean AND and OR operators.

You can also sort the objects in ascending or descending order.

The list is filtered as specified to show only the matching items in the page.

7

To adjust or customize the information display in the content pane, click ⋮ in the column heading and select one of the following:

- Clear sorting—reset the sorting criteria to the defaults
- Clear filters—clear all filters that are applied

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Manage columns...—specify which columns are displayed

8

To refresh the display, click ↻ in the window header.

Directory operations

9

To create a directory at the same level as the current directory:

1. Click ＋ in the Root Directory List pane.
   The Create Root Directory form opens.
2. Specify a directory name.
3. Click **CREATE**. The new directory is added to the Root Directory List.

10

To create a child directory of a listed root directory:

1. Select the directory in the Root Directory List pane or directory list.
2. Click ⋮, **Create Directory** beside the directory.
   The Create Directory form opens.
3. Specify a directory name.
4. Click **CREATE**. The directory is created.

11

To rename a directory:

1. Select the directory in the Directory List.
2. Click ⋮, **Rename Directory** beside the directory.
   The Update Directory Name form opens.
3. Specify a directory name.
4. Click **RENAME**. The directory is renamed.

12

To import a file to the directory:

1. Select the directory in the Directory List.
2. Click ⋮, **Import File** beside the directory, or click ⤓ above the content pane.
   A file browser window opens.
3. Click Open. The file is imported to the current directory.

13

To delete a directory:

1. Select the directory in the Directory List.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Click ⋮, **Delete Directory** beside the directory.
   The Delete Directory Name form opens.
3. Click **DELETE**. The directory is deleted.

14

To export a list of directory contents to a file:

1. Select the directory in the Directory List.
2. Click ⋮, **Export selected**, *format* beside the content-pane header.
   The directory listing is saved as a file in your browser downloads folder.

File operations

15

To rename a file:

1. Click ⋮, **Rename File** beside the file.
   The Update File form opens.
2. Specify a new name.
3. Click **RENAME**. The file is renamed.

16

To import a file to a directory:

1. Select the directory in the Directory List.
2. Click ⋮, **Import File** beside the directory, or click ⤓above the content pane.
   A file browser window opens.
3. Click Open. The file is imported to the directory.

17

To download a file, click ⋮, **Download File** beside the file:
The file is saved in your browser downloads folder.

18

To delete a file:

1. Click ⋮, **Delete File** beside the file.
   The Delete File form opens.
2. Click **DELETE**. The file is deleted.

19

To view a file:

1. Click ⋮, **View File** beside the file.
   A File Viewer form opens and displays the file content.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. When you are finished viewing the content, click OK to close the form.

Using the global search function

20

To search for File Server file or directory by name:

Note: Searches are case-insensitive.

1. Type part or all of the object name in the search window at the top right of the File Server page, and then click .

   The Directory List is hidden, and the matching files and directories are listed.

   The global search results are across all files and directories.

2. As required, click beside an object to choose an action to perform on the object.

   Directory object:
   - Open Directory—display the directory content
   - Create Directory—create a child directory
   - Import File—import a file to the directory, as described in Step 12
   - Delete Directory—remove the directory from the File Server

   File object:
   - Open Parent Directory—open the directory that contains the file
   - Import File—import a file to the directory, as described in Step 16
   - Download File—download the file
   - Delete File—remove the file from the File Server
   - View File—display the file content

3. To close the global search function and return to the File Server home view, click beside the search window.

   The search window closes, and the Directory List and content pane are displayed.

END OF STEPS

5.4 How do I configure file purge policies?

5.4.1 Purpose

Use this procedure to modify the configuration of the global file purge policy, and to manage override policies.

5.4.2 Steps

1

From the **NSP Menu**, select **File Server**.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The left pane displays the Directory List; the content pane, which is adjacent, lists the objects in the selected directory, and the collapsible Info pane at the right side displays information about the currently selected file or directory.

2

On the File Server page, click **File Server Settings**.

The File Server Settings form opens with the Global Policy settings displayed.

3

To update the global policy:

1. Configure the following parameters, as required:
   - **Used Threshold %**—percentage of disk space at which file are purged
   - **Cleanup %**—percentage of total disk space purged on the file server when critical threshold is reached
   - **Retention Period**—number of days or hours before files are purged

     Select the **Days** or **Hours** option and then set the **Interval**.
2. If required, click **Add Ignore List**

   The Ignore List window opens.
3. To exclude a file specification from the global purge settings, choose a directory and click Add.

   The directory is excluded from the global purge policy.

   See 5.2.2 “Ignore Lists” (p. 78) for information.

   Note: If required, you can apply specific purge settings to the excluded directory using an override policy, as described in Step 4.
4. To remove a file specification from the **Ignore List**, choose a directory in the Ignore List window.

   The directory contents are displayed in the right content pane.

   Choose a directory in the right content pane, and click on the right side of the item.
5. Click SAVE.

4

To create an override policy, perform the following steps. You can add multiple directories to an override policy.

1. In the Override Policies panel, click **Add Directory**. The Select Directory form opens.
2. In the **Search Directories** field, type all or part of the directory name and choose from the auto-complete list.

   The directory is added to the list.
3. Configure the following parameters:
   - **Allocated space**—disk space allocated to the directory and subdirectories
   - **Used Threshold %**—percentage of disk space at which files are purged

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- **Cleanup %**—percentage of total disk space purged on the file server when critical threshold is reached
- **Retention Period**—number of days or hours before files are purged

  Select the **Days** or **Hours** option and then set the **Interval**.

4. If required, click **Add Ignore List**

   The Ignore List window opens.

5. Choose one or more file specifications to exclude from the override policy purge settings; see 5.2.2 “Ignore Lists” (p. 78) for information.

   The file specification that you choose is used for a string search in the directory and subdirectories. For example, if the override policy names the /MyDir directory and you add an override for /MyDir/Temp, each file and subdirectory below /MyDir whose name begins with Temp is excluded from the override policy.

6. Click **Add & Save Directory**.

5

To modify an override policy:

1. Click ⋮ on the policy line and choose **Edit**.

   The Update Purge Policy window opens.

2. Modify the policy settings, as required.
3. Click UPDATE DIRECTORY.

   The policy is updated.

6

To disable an override policy, click ⋮ on the policy line and choose **Disable**.

The policy is disabled, the policy Status changes from Enabled to Disabled, and the global policy settings apply to the directory named in the policy.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part II: NSP security administration

Overview

Purpose

This part of the *NSP System Administrator Guide* describes how to configure and manage NSP platform, user, and network security.

Contents

Chapter 6, SELinux administration	87
Chapter 7, TLS administration	111
Chapter 8, NSP user security	155
Chapter 9, Classic management security	215
Chapter 10, Classic management NE security	275

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6 SELinux administration

6.1 Overview

6.1.1 Purpose

This chapter describes how to implement, manage, and troubleshoot SELinux in an NSP deployment.

6.1.2 Contents

6.1 Overview	87
Deploying SELinux	88
6.2 What is SELinux?	88
6.3 How do I enable SELinux on an NSP deployer VM?	89
6.4 How do I enable SELinux in an NSP cluster?	91
SELinux for Classic Management	95
6.5 What does enabling NFM-P SELinux involve?	95
6.6 How do I enable SELinux on the NFM-P?	95
6.7 How do I enable SELinux enforcing mode for the NFM-P?	100
SELinux troubleshooting	103
6.8 What does NSP SELinux troubleshooting involve?	103
6.9 How do I switch between SELinux modes on NSP system components?	103
6.10 How do I troubleshoot SELinux on NSP system components?	105
6.11 How do I troubleshoot SELinux on the NFM-P?	107

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Deploying SELinux

6.2 What is SELinux?

6.2.1 Introduction

For greater system security, you can enable RHEL SELinux on NSP components. SELinux logs user operations in Application Visibility and Control, or AVC messages that are stored in local logs. SELinux has two modes, permissive and enforcing; the support for each is described in 6.2.2 “SELinux support scope” (p. 88).

See the RHEL documentation for comprehensive SELinux configuration and implementation information.

Note: The SELinux policies for the NSP product are to be applied only to the NSP product and the RHEL OS packages listed in the *NSP Installation and Upgrade Guide*. Any SELinux denials for other software packages are not the responsibility of Nokia.

SELinux permissive mode

No SELinux policy is enforced in permissive mode, and no operations are denied. However, SELinux does log AVC messages while in permissive mode. AVC messages may be of use for troubleshooting, debugging, and SELinux policy improvements. An AVC message is logged each time a violation occurs.

SELinux enforcing mode

In enforcing mode, SELinux enforces the policies specified in the NSP SELinux configuration, and logs AVC messages as required.

Restricted root-user access

If restricted root-user access is enabled, each SELinux command in the following procedures must be run by the NSP admin user and prefaced with ‘sudo’.

6.2.2 SELinux support scope

The procedures in this section describe enabling SELinux on the following:

- NSP deployer VM
- NSP cluster VM

Note: An NSP auxiliary database supports SELinux only in permissive mode, which is enabled by default.

“SELinux for Classic Management” (p. 95) describes enabling SELinux on the following, which support SELinux enforcing mode:

- NFM-P main server
- NFM-P main database
- NFM-P auxiliary server

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6.3 How do I enable SELinux on an NSP deployer VM?

6.3.1 Purpose

Perform this procedure to enable SELinux on the NSP deployer VM in an NSP cluster.

Note: You must enable permissive mode on the NSP deployer VM before you can enable enforcing mode on the NSP deployer VM.

Note: You require root user privileges on the NSP deployer VM.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

6.3.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/tools/selinux/tools/bin ↵
```

Check for required OS packages

4

Enter the following:

```
# ./selinuxenable.sh -c ↵
```

Any missing OS packages required by SELinux are listed.

5

If the message indicates that one or more required SELinux packages are not installed, enter the following:

```
# dnf -y install package_1 package_2 ... package_n ↵
```

where *package_1 package_2* ... *package_n* are the names of the listed packages

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The packages are installed.

Enable permissive mode

6

./selinuxenable.sh -p ↵

The SELinux mode is set to permissive.

Apply SELinux labels

7

Enter the following:

cd /opt/nsp/nsp-k8s-deployer-*release-ID*/tools ↵

8

Enter the following:

selinux/installer/bin/nsp-selinux-config.bash ↵

The script loads the required AVC policy, k3s_nsp_domain.pp, and labels the files and directories named in the policy.

9

Enter the following to back up the system audit logs:

cp /var/log/audit/audit.log* *backup_location* ↵

where *backup_location* is a secure location on a separate station

10

Enter the following to delete the system audit logs and thereby clear the SELinux AVC history:

rm -f /var/log/audit/audit.log* ↵

11

Enter the following:

systemctl reboot ↵

The station reboots.

After the reboot, the SELinux labels take effect as SELinux runs in targeted permissive mode in the nsp_domain_t domain.

12

After the reboot, enter the following to verify that the required processes are running in the nsp_domain_t domain:

ps -aefZ | grep -v grep | egrep 'k3s|harbor|traefik|coredns|provisioner|registry'↵

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Process entries like the following are listed:

```
system_u:system_r:nsp_domain_t:s0 process_description
```

13

If any listed entry does not include nsp_domain_t, contact technical support for assistance.

14

Enter the following to verify that the policy file is loaded.

```
# semodule -l | grep k3s_nsp_domain ↵
```

The policy file is listed, as shown below:

```
k3s_nsp_domain
```

15

If the k3s_nsp_domain policy is not listed, contact technical support for assistance.

16

Close the open console windows.

END OF STEPS

6.4 How do I enable SELinux in an NSP cluster?

6.4.1 Purpose

Perform this procedure to enable SELinux on the member nodes of an NSP cluster.

Note: You must enable permissive mode on all NSP cluster nodes before you can enable enforcing mode on the nodes.

Note: You require root user privileges on each NSP cluster node.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

6.4.2 Steps

1

Perform Step 3 to Step 11 on each node in the NSP cluster.

2

Go to Step 12.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Individual node configuration

3

Log in as the root user on the NSP cluster node.

4

Open a console window.

5

Enter the following:

```
# cd /opt/nsp/nsp-deployer/tools/selinux/tools/bin ↵
```

Check for required OS packages

6

Enter the following:

```
# ./selinuxenable.sh -c ↵
```

Any missing OS packages required by SELinux are listed.

7

If the message indicates that one or more required SELinux packages are not installed, enter the following:

```
# dnf -y install package_1 package_2 ... package_n ↵
```

where *package_1 package_2* ... *package_n* are the names of the listed packages

The packages are installed.

Enable permissive mode

8

Enter the following:

```
# ./selinuxenable.sh -p ↵
```

The SELinux mode is set to permissive.

Apply SELinux labels

9

Enter the following:

```
# /opt/nsp/nsp-deployer/tools/selinux/installer/bin/nsp-selinux-config.bash ↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The script loads the required AVC policy, k8s_nsp_domain.pp, and labels the files and directories named in the policy.

10

Enter the following to back up the system audit logs:

```
# cp /var/log/audit/audit.log* backup_location ↵
```

where *backup_location* is a secure location on a separate station

11

Enter the following to delete the system audit logs and thereby clear the SELinux AVC history:

```
# rm -f /var/log/audit/audit.log* ↵
```

Restart NSP cluster

12

Perform 12.8 “How do I stop an NSP cluster?” (p. 371) to gracefully shut down the NSP cluster and preserve the cluster data.

13

Enter the following:

```
# systemctl reboot ↵
```

The node reboots.

After the reboot, the SELinux labels take effect as SELinux runs in targeted permissive mode in the nsp_domain_t domain.

14

After the reboot, enter the following to verify that the required processes are running in the nsp_domain_t domain:

```
# ps -aefZ | egrep 'kube-apiserver | kube-scheduler |
kube-controller-manager | /usr/local/bin/etcd |
/usr/local/bin/kube-proxy | /usr/local/bin/kubelet|/kube-state-metrics
| /usr/bin/kube-controllers' | egrep -v 'grep' ↵
```

Process entries like the following are listed:

```
system_u:system_r:nsp_domain_t:s0 process_description
```

15

If any listed entry does not include nsp_domain_t, contact technical support for assistance.

16

Enter the following to verify that the policy file is loaded.

```
# semodule -l | grep k8s_nsp_domain ↵
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The policy file is listed, as shown below:

```
k8s_nsp_domain
```

17

Start the NSP cluster; perform 12.9 “How do I start an NSP cluster?” (p. 373).

18

Close the open console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

SELinux for Classic Management

6.5 What does enabling NFM-P SELinux involve?

6.5.1 Description

6.6 “How do I enable SELinux on the NFM-P?” (p. 95) describes how to enable SELinux on NFM-P components in permissive mode.

When all components are fully operational in permissive mode, you can use 6.7 “How do I enable SELinux enforcing mode for the NFM-P?” (p. 100) to enable enforcing mode on each component, if required.

6.6 How do I enable SELinux on the NFM-P?

6.6.1 Purpose

CAUTION

Service Disruption

Enabling SELinux in a standalone or redundant NFM-P system creates a network management outage. A standalone system requires a full shutdown and restart; a redundant system requires one or more server activity switches that each may cause a brief service interruption.

Perform the procedure only during a scheduled maintenance period of sufficient duration with the guidance of technical support.

Perform this procedure to enable SELinux on the components of an NFM-P system. You must perform the procedure on each main server, main database, and auxiliary server station.

Note: You must enable permissive mode on each component before you can enable enforcing mode on the components.

Note: You require the following user privileges:

- on each main and auxiliary server station — root, nsp
- on each main database station — root

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6.6.2 Steps

Check for required OS packages

1

Before you can enable SELinux on a station, you must ensure that the required RHEL OS packages are installed.

Perform the following steps on each main server, main database, and auxiliary server station.

1. Log in to the station as the root user.
2. Open a console window.
3. Enter the following:

   # **cd /opt/nsp/nfmp/config/selinux/tools/bin** ↵
4. Enter the following:

   # **./selinuxenable.sh -c** ↵

   Any missing OS packages required by SELinux are listed.
5. If the message indicates that one or more required SELinux packages are not installed, enter the following:

   # **dnf -y install *package_1 package_2 ... package_n*** ↵

   where *package_1 package_2 ... package_n* are the names of the listed packages

   The packages are installed.

Close client sessions

2

Close the open NFM-P GUI and XML API client sessions, as required.

1. Open a GUI client using an account with security management privileges, such as admin.
2. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
3. Click on the Sessions tab.
4. Click Search. The form lists the open GUI and XML API client sessions.
5. Identify the GUI session that you are using based on the value in the Client IP column.
6. Select all sessions except for the following:
   - the session that you are using
   - the sessions required to monitor the network during a redundant system upgrade
7. Click Close Session.
8. Click Yes to confirm the action.
9. Click Search to refresh the list and verify that only the required sessions are open.
10. Close the NFM-P User Security - Security Management (Edit) form.
11. Close your GUI client.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12. Sign out of the NSP UI, if you are signed in.

3

If the NFM-P system is standalone:

1. Perform Step 5 to Step 10 on the main server, main database, and auxiliary server.
2. Go to Step 13.

4

If the NFM-P system is redundant:

1. Perform Step 5 to Step 12 on the standby server complex.

   After this step, the initial standby server complex is the new primary complex.
2. Perform Step 5 to Step 10 on the initial primary server complex, which is the new standby server complex.
3. If you want to restore the initial primary and standby roles of the server complexes, go to Step 11. Otherwise, go to Step 13.

Stop system components

5

Stop the main server.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```
4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```
5. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.
6. Enter the following to switch to the root user:

   ```
   bash$ su - ↲
   ```

6

Stop the Oracle proxy and database services.

1. Log in to the database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# systemctl stop nfmp-oracle-proxy.service ↵
```

4. Enter the following to stop the main database:

```
# systemctl stop nfmp-main-db.service ↵
```

7

If the system includes one or more auxiliary servers, stop each auxiliary server.

1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:

```
bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop ↵
```

The auxiliary server stops.

Enable SELinux permissive mode

8

Enter the following as the root user on each main server, main database, and auxiliary server station:

```
# /opt/nsp/nfmp/config/selinux/tools/bin/selinuxenable.sh -p ↵
```

Apply SELinux labels and reboot

9

Perform the following steps as the root user on each main server, main database, and auxiliary server station.

1. Enter the following:

```
# cd /opt/nsp/nfmp/config/selinux/installer/bin ↵
```

2. Enter the following:

```
# ./nsp-selinux-config.bash ↵
```

3. Enter the following to back up and then remove the system audit logs:

```
# ./backup-rm-auditlogs.bash backup_dir ↵
```

where *backup_dir* is an optional backup location; if omitted, the audit logs are saved in the following directory:

/opt/nsp/nfmp/config/selinux/installer/log

The station reboots.

After the reboot, the SELinux labels take effect as SELinux runs in targeted permissive mode in the nsp_domain_t domain.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Verify system startup

10

After each station is rebooted, verify that the main server, main database, and auxiliary servers are operational.

Note: If any command in a substep indicates that the component is not yet operational, wait one minute and then re-issue the command.

1. Enter the following as the root user on the main database station:

   `# systemctl status nfmp-main-db.service` ↵

   If the command output includes the following, the database is operational:

   `Active: active (running) since time`

2. Enter the following as the root user on the main database station:

   `# systemctl status nfmp-oracle-proxy.service` ↵

   If the command output includes the following, the database proxy is operational:

   `Active: active (running) since time`

3. Enter the following as the nsp user on the main server station:

   `bash$ ./nmsserver.bash appserver_status` ↵

   If the command output includes the following, the main server is operational:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

4. On each auxiliary server station, enter the following as the nsp user:

   `bash$ ./auxnmsserver.bash auxappserver_status` ↵

   If the command output includes the following, the auxiliary server is operational:

   ```
   Auxiliary Server process is running.  See auxnms_status for more
   detail.
   ```

Switch redundancy roles

11

If automatic database realignment is not enabled, perform a database switchover.

1. As the nsp user on the main server station, enter the following:

   `bash$ /opt/nsp/nfmp/server/nms/bin/switchoverdb.bash -u username -p password` ↵

   where *username* and *password* are the login credentials of an NFM-P user with the required privilege level and scope of command

   The script displays the following confirmation message:

   ```
   The standby database will become the new primary database, and the
   old primary will become the new standby. Do you want to proceed?
   (YES/no) :
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Enter the following to initiate the switchover:

   YES ↵

   The NFM-P server initiates a database switchover. Progress is indicated by a rolling display of dots in the console window. The database switchover is complete when the CLI prompt reappears.

12

Enter the following to perform a server activity switch:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash force_restart ↵
```

The server activity switch begins. The standby main server restarts as the primary main server, and the primary restarts as the standby.

13

Close the open console windows.

END OF STEPS

6.7 How do I enable SELinux enforcing mode for the NFM-P?

6.7.1 Purpose

CAUTION

Potential Security Risk

Enabling SELinux enforcing mode when any AVCs remain unresolved may pose a security risk.

Before you attempt to enable enforcing mode, you must resolve any AVCs associated with the nsp_domain_t domain that are raised during a soak period in permissive mode.

It is strongly recommended that the system run in permissive mode for at least seven days with no nsp_domain_t AVCs on any NFM-P main server, main database, or auxiliary server.

Perform this procedure to enable SELinux enforcing mode in an NFM-P system.

Note: You must perform the procedure on each component that supports SELinux enforcing mode, as listed in 6.2.2 “SELinux support scope” (p. 88).

Note: You must enable permissive mode on each component, as described in 6.6 “How do I enable SELinux on the NFM-P?” (p. 95), before you can enable enforcing mode on the components.

Note: You do not need to stop any NFM-P processes in order to switch from permissive to enforcing mode.

Note: You require root user privileges on each station.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

6.7.2 Steps

1

Log in to the component station as the root user.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/nfmp/config/selinux/tools/bin ↵
```

4

Enter the following to show the number of system and NSP-domain AVCs:

```
# ./setroubleshoot.bash collect-avcs ↵
```

The following messages are displayed:

```
Generating RAW AVC file...
+ Total Number of distinct AVCs: n
    + Number of AVCS related to nsp_domain: n
```

5

If the command returns any NSP-domain AVCs, enter the following:

```
# ./setroubleshoot.bash resolve-nsp-avcs my_policy ↵
```

where *my_policy* is a file name other than nsp_domain that does not include ‘module’

A policy module file with a .te extension is created in /opt/nsp/nfmp/config/selinux/tools/bin/tmp/policy.

6

WARNING

Extreme Security Risk

The policy module file generated in Step 5 must be reviewed by an experienced SELinux user before the file is loaded in a subsequent step, or system security may be seriously compromised.

The reviewer must ensure that the file does not include any entry that may constitute a security risk to your system.

Ensure that the generated policy module file passes a security review.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Enlist an experienced SELinux user to review the policy module file.
2. If the review reveals any AVCs that need to be included in the generic NSP SELinux policy, the reviewer must open a support ticket and include the SELinux logs data generated by running the following script:

   /opt/nsp/nfmp/config/selinux/tools/bin/cgselinuxlogs.sh
3. Make note of the policy created in Step 5 in the event that the experienced SELinux user needs to modify or remove the policy in the future. Maintenance of the policy is the responsibility of the SELinux user.

Note: If the review reveals any AVC issues, you must not proceed to the next step until the AVC issues are resolved.

7

Enter the following:

```
# cd /opt/nsp/nfmp/config/selinux/tools/bin/tmp/policy ↵
```

8

Enable enforcing mode.

1. Enter the following:

   ```
   # cd /opt/nsp/nfmp/config/selinux/tools/bin ↵
   ```
2. ```
   # ./selinuxenable.sh -e ↵
   ```

SELinux is enabled in enforcing mode.

9

Enter the following:

```
# getenforce ↵
```

The SELinux mode is displayed.

10

View the command output to verify that SELinux is enabled in enforcing mode.

11

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms
```

SELinux troubleshooting

6.8 What does NSP SELinux troubleshooting involve?

6.8.1 Description

In the event that a system or component in SELinux enforcing mode has functional issues and an AVC is present, a change to permissive mode, as described in 6.9 “How do I switch between SELinux modes on NSP system components?” (p. 103), may resolve the issue. If enabling permissive mode resolves the issue, and the AVC is in the NSP domain, it is strongly recommended that you raise a support ticket to report the AVC.

6.10 “How do I troubleshoot SELinux on NSP system components?” (p. 105) and 6.11 “How do I troubleshoot SELinux on the NFM-P?” (p. 107) describe further troubleshooting actions that you can pursue to resolve an SELinux issue.

6.9 How do I switch between SELinux modes on NSP system components?

6.9.1 Purpose

CAUTION

Potential Security Risk

Enabling SELinux enforcing mode when any AVCs remain unresolved may pose a security risk.

Before you attempt to enable enforcing mode, you must resolve any AVCs associated with the nsp_domain_t domain that are raised during a soak period in permissive mode.

It is strongly recommended that the system run in permissive mode for at least seven days with no nsp_domain_t AVCs on any NSP component.

Perform this procedure to switch between SELinux permissive and enforcing modes on one or more of the following:

- NSP deployer VM
- NSP cluster nodes

Note: You do not need to stop any NSP processes in order to switch between SELinux modes.

Note: You require root user privileges on a station to switch SELinux modes.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

6.9.2 Steps

1

Log in as the root user on the station.

2

Open a console window.

3

Enter one of the following, depending on the NSP component type:

a. NSP deployer VM:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/tools/selinux/tools/bin ↲
```

b. NSP cluster node:

```
# cd /opt/nsp/nsp-deployer/tools/selinux/tools/bin ↲
```

4

To switch from permissive to enforcing mode, enter the following:

```
# ./selinuxenable.sh -e ↲
```

The following messages are displayed, and the SELinux mode changes to enforcing:

```
Checking that the required selinux packages are installed.
Required packages installed
selinux currently enabled in permissive mode, change to enforcing
mode.
```

5

To switch from enforcing to permissive mode, enter the following:

```
# ./selinuxenable.sh -p ↲
```

The following messages are displayed, and the SELinux mode changes to permissive.

```
Checking that the required selinux packages are installed.
Required packages installed
selinux currently enabled in enforcing mode, change to permissive
mode.
```

6

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6.10 How do I troubleshoot SELinux on NSP system components?

6.10.1 Purpose

Perform this procedure to list and resolve any open AVCs on one of the following:

- NSP deployer VM
- NSP cluster nodes
- NSP auxiliary database

Note: You require root user privileges on a station to switch SELinux modes.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

6.10.2 Steps

1

Log in as the root user on the station.

2

Open a console window.

3

Enter one of the following, depending on the NSP component type:

a. NSP deployer VM:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/tools/selinux/tools/bin ↵
```

b. NSP cluster node:

```
# cd /opt/nsp/nsp-deployer/tools/selinux/tools/bin ↵
```

4

Enter the following to show the number of system and NSP-domain AVCs:

```
# ./setroubleshoot.bash collect-avcs ↵
```

The following messages are displayed:

```
Generating RAW AVC file...
+ Total Number of distinct AVCs: n
    + Number of AVCS related to nsp_domain: n
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

If the number of nsp_domain AVCs is zero, go to Step 9.

6

Enter the following to generate an AVC list file:

```
# ./setroubleshoot.bash resolve-nsp-avcs AVC_list ↵
```

where *AVC_list* is a name to assign to the generated file

The following messages are displayed, and an AVC list file with a .te extension is created in the directory described in the messages:

```
Generating RAW AVC file...
nsp_domain_t AVCs present... generating te file
Generated /path/AVC_list.te file
IMPORTANT: The /path/tmp/policy/AVC_list/AVC_list.te file generated by this script must be reviewed by an experienced SELinux user before loading
You must ensure that the /path/tmp/policy/AVC_list/AVC_list.te file does not include entries that may constitute a security risk to your system.
```

7

WARNING

Extreme Security Risk

The generated file must be reviewed by an experienced SELinux user before the file is loaded in a subsequent step, or system security may be seriously compromised.

The reviewer must ensure that the file does not include any entry that may constitute a security risk to your system.

Enlist an experienced SELinux user to review the AVC list file.

8

If the review reveals any AVCs that need to be included in the generic NSP SELinux policy, perform the following steps.

1. Enter the following to capture the local SELinux log files for further analysis by Nokia:

   ```
   # ./cgselinuxlogs ↵
   ```

   Messages like the following are displayed:

   ```
   Creating log file... /path/selinux
   Deleting previous generated selinux logs in /path/selinux
   Running selinux_capture_logs.sh, please wait (have patience..).
   ...
   ```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Log files going to directory /path/selinux
.
.
.
Provide the following to Nokia for review:
/tmp/nspselinux/selinuxLogsselinux-station_descriptor-timestamp.
tar.gz
```

2. Direct the SELinux user to make note of the generated file in the event that the policy requires modification in the future.

   Note: Maintenance of the policy is the responsibility of the SELinux user.

3. Direct the SELinux user to open a Nokia support ticket that includes the generated /tmp/nspselinux/selinuxLogsselinux-*station_descriptor-timestamp*.tar.gz file.

9

Close the console window.

END OF STEPS

6.11 How do I troubleshoot SELinux on the NFM-P?

6.11.1 Purpose

Perform this procedure if SELinux enforcing mode is enabled and you suspect that SELinux is affecting NFM-P operation.

Note: The procedure applies only to the NFM-P components that support SELinux enforcing mode, as listed in 6.2.2 “SELinux support scope” (p. 88).

Note: You must perform the procedure on each NFM-P station that has SELinux enforcing mode enabled.

Note: You require root user privileges on each station.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

6.11.2 Steps

1

Log in as the root user on the standalone or primary NFM-P main server station.

2

Open a console window.

3

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Enter the following:

```
# cd /opt/nsp/nfmp/config/selinux/tools/bin ↵
```

4

Switch to SELinux permissive mode.

Note: The NFM-P main server can remain running during the switch from enforcing to permissive mode.

1. Enter the following:

   ```
   # ./selinuxenable.sh -p ↵
   ```

2. Enter the following to verify that SELinux is in permissive mode:

   ```
   # getenforce ↵
   ```

   The SELinux mode is displayed.

3. View the command output to verify that SELinux is enabled in permissive mode.

5

Enter the following to show the number of system and NSP-domain AVCs:

```
# ./setroubleshoot.bash collect-avcs ↵
```

The following messages are displayed:

```
Generating RAW AVC file...
+ Total Number of distinct AVCs: n
    + Number of AVCS related to nsp_domain: n
```

6

If the command returns any NSP-domain AVCs, enter the following:

```
# ./setroubleshoot.bash resolve-nsp-avcs my_policy ↵
```

where *my_policy* is a file name other than nsp_domain that does not include ‘module’

A policy module file with a .te extension is created in /opt/nsp/nfmp/config/selinux/tools/bin/tmp/policy.

7

WARNING

Extreme Security Risk

The policy module file generated in Step 6 must be reviewed by an experienced SELinux user before the file is loaded in a subsequent step, or system security may be seriously compromised.

The reviewer must ensure that the file does not include any entry that may constitute a security risk to your system.

Ensure that the generated policy module file passes a security review.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Enlist an experienced SELinux user to review the policy module file.
2. If the review reveals any AVCs that need to be included in the generic NSP SELinux policy, the reviewer must open a support ticket and include the SELinux logs data generated by running the following script:

   /opt/nsp/nfmp/config/selinux/tools/bin/cgselinuxlogs.sh
3. Make note of the policy created in Step 6 in the event that the experienced SELinux user needs to modify or remove the policy in the future. Maintenance of the policy is the responsibility of the SELinux user.

Note: If the review reveals any AVC issues, you must not proceed to the next step until the AVC issues are resolved.

8

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7 TLS administration

7.1 Overview

7.1.1 Purpose

This chapter describes the required operations required for NSP TLS administration, such as renewing expired certificates.

7.1.2 Contents

7.1 Overview	111
What is NSP TLS administration?	113
7.2 NSP TLS administration overview	113
7.3 Managing Kubernetes infrastructure TLS	114
7.4 Managing NSP system TLS	115
NSP Kubernetes TLS administration procedures	116
7.5 How do I update the K3s certificate for an NSP deployer VM?	116
7.6 How do I update the Kubernetes registry TLS certificate?	117
7.7 How do I update nsp_kubeconfig on the NSP deployer host?	119
7.8 How do I add Kubernetes load balancer external IP addresses?	119
NSP cluster TLS administration procedures	121
7.9 How do I list the NSP Kubernetes secrets?	121
7.10 How do I view the Kubernetes secret content?	122
7.11 How do I update the NSP issuer TLS certificates?	123
7.12 How do I update the custom NSP server TLS certificates?	127
7.13 How do I add an NSP Kubernetes secret?	130
7.14 How do I recreate the NSP Kubernetes secrets?	132
7.15 How do I back up the NSP Kubernetes secrets?	138
7.16 How do I restore the NSP Kubernetes secrets?	139
7.17 How do I update the Keycloak OpenSearch client secret?	140
NSP component TLS configuration	142
7.18 How do I configure an NSP auxiliary database to request the NSP TLS certificate?	142

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.19 How do I configure an NFM-P main server to request the NSP TLS certificate?	143
7.20 How do I configure an NFM-P auxiliary server to request the NSP TLS certificate?	146
7.21 How do I enable TLS for NFM-P XML API clients?	149
7.22 How do I disable TLS for NFM-P XML API clients?	152

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

What is NSP TLS administration?

7.2 NSP TLS administration overview

7.2.1 Managing NSP TLS certificates

NSP TLS certificate renewal or replacement is required when:

- a certificate nears or reaches expiry
- a component is added to the NSP system
- an NSP component is replaced
- an NSP component address changes
- responding to a CA or algorithm compromise

Required NSP cluster certificates

An NSP cluster uses the following TLS certificates:

- Kubernetes infrastructure certificates, applied to:
  - Kubernetes registry
  - NSP deployer VM
  - NSP cluster control plane
- issuer certificates, applied to:
  - internal NSP subsystem and service endpoints
  - external-facing NSP application endpoints
- server certificates, applied to:
  - NSP cluster gateway for client access
  - mediation interfaces

7.2.2 Storage in Kubernetes secrets

The NSP TLS certificates are stored in Kubernetes secrets to prevent the exposure of high-risk security information. You use an NSP utility to manage the secrets and certificates in the secrets.

To show basic information about the installed secrets such as the namespaces and ages, see 7.9 “How do I list the NSP Kubernetes secrets?” (p. 121).

To show the content of each secret, see 7.10 “How do I view the Kubernetes secret content?” (p. 122).

7.2.3 Support for deprecated TLS versions

An external system such as an OSS client may use an older, deprecated TLS version. For compatibility with such a client, you can enable older TLS versions by setting the tlsv1ProtocolsEnabled parameter in the nsp-config.yml file.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.2.4 TLS expiry notifications

The NSP checks the expiry date of a monitored TLS certificate during initialization, and every 24 hours thereafter. After an NSP TLS certificate expires, the NSP cluster continues to operate, but functions that depend on secure communication are unavailable.

When a certificate expires or approaches expiry, the NSP raises one of the following server or internal certificate alarms:

- Warning, if the certificate is to expire within 30 days of the current time
- Critical, if the certificate is to expire within 7 days of the current time
- Critical, if the certificate is expired

Note: The NSP raises one alarm per certificate.

Note: The alarms for internal or external NSP certificate expiry do not clear automatically.

Note: No alarm is raised for an expiring or expired NSP Kubernetes infrastructure certificate.

Note: The Days Remaining value in an expiry alarm is based on the number of complete 24-hour periods until the certificate expiry time. If fewer than 24 hours remain until expiry, the Days Remaining value is zero; however, the NSP does not raise an alarm about the certificate expiry until the next periodic check, 24 hours later.

7.11 “How do I update the NSP issuer TLS certificates?” (p. 123) describes how to replace the internal TLS certificate, the external certificate, or both, in an NSP system.

7.3 Managing Kubernetes infrastructure TLS

7.3.1 Description

The NSP Kubernetes infrastructure certificates undergo automatic scheduled renewal, but manual renewal or replacement options are also available, as described below.

NSP Kubernetes registry

An NSP cluster communicates with the local Kubernetes registry to pull container images and Helm charts. You can replace the Kubernetes registry certificate, if required, as described in 7.6 “How do I update the Kubernetes registry TLS certificate?” (p. 117).

NSP deployer VM

The NSP automatically renews the NSP deployer VM TLS certificates twice annually, based on an internal schedule; no operator action is required.

You can, however, manually update the K3s certificate on the NSP deployer VM, as may be required for security reasons, or, for example, if the NSP deployer VM is shut down at the scheduled renewal time. See 7.5 “How do I update the K3s certificate for an NSP deployer VM?” (p. 116) for information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP cluster VMs

The TLS certificates that secure the NSP cluster VM control plane renew automatically and silently monthly.

No alarm is raised for the expiry or renewal; however, the renewal action is logged in the /var/log/messages file on the NSP cluster host. The following is the starting log entry for a renewal operation:

```
timestamp node1-3 systemd: Starting Renew K8S control plane
certificates...
```

7.4 Managing NSP system TLS

7.4.1 Secrets management

The following procedures describe how to manage the Kubernetes secrets and associated TLS certificates in an NSP cluster:

- internal and external issuer certificates—7.11 “How do I update the NSP issuer TLS certificates?” (p. 123)
- custom certificate for NSP client access—7.12 “How do I update the custom NSP server TLS certificates?” (p. 127)
- new secret, for example, to support a new mediation interface—7.13 “How do I add an NSP Kubernetes secret?” (p. 130)
- new set of secrets for cluster recreation—7.14 “How do I recreate the NSP Kubernetes secrets?” (p. 132)

7.4.2 Updating TLS certificates on NSP components

The procedures in “NSP component TLS configuration” (p. 142) describe how to configure NSP components deployed outside an NSP cluster, for example, the NFM-P or an NSP auxiliary database, to retrieve the required TLS certificates from the NSP cluster.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP Kubernetes TLS administration procedures

7.5 How do I update the K3s certificate for an NSP deployer VM?

7.5.1 Purpose

Under normal operating conditions, the NSP deployer VM TLS certificate renews automatically, and no manual action is required. However, if the certificate is corrupt, the auto-renewal fails, or as a regular security exercise, you can use the following steps to update the certificate manually.

Note: You require root user privileges on the NSP deployer VM.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

7.5.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/nsp-registry-release-ID/bin ↵
```

4

Enter the following to update the certificate:

```
# ./nspregistryctl update --k3s-cert ↵
```

The NSP updates the certificate and creates a new renewal schedule based on the current time.

5

Enter the following to ensure that all pods are running after the certificate update:

Note: The nsp deployer log file is /var/log/nspdeployerctl.log.

```
# kubectl get pods -A ↵
```

The status of each pod is listed; the NSP cluster is operational when each pod STATUS value is Running or Completed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

If the cluster fails to become operational after the typical initialization period, record the cluster status and contact technical support.

7

When the cluster is operational, close the console window.

END OF STEPS

7.6 How do I update the Kubernetes registry TLS certificate?

7.6.1 Purpose

CAUTION

Potential Service Disruption

Performing the procedure restarts the containerd service, which is temporarily service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance window under the guidance of technical support.

Under normal operating conditions, the NSP Kubernetes registry certificate renews automatically, and no manual action is required. However, if the certificate is corrupt, the auto-renewal fails, or as a regular security exercise, you can use the following steps to update the certificate manually.

Note: You require root user privileges on the NSP deployer VM.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

7.6.2 Steps

1

Open a terminal session to the NSP deployer VM

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/nsp-registry-release-ID/bin ↵
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Enter the following to update the certificate:

```
# ./nspregistryctl update -c ↵
```

The NSP container registry certificate is updated.

5

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

6

Enter the following to update the certificate on each NSP cluster member:

```
# ./nspk8sctl update -r ↵
```

The update is performed, and the contained service restarts.

7

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# Export KUBECONFIG /opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↵
```

8

Open a console window.

9

Enter the following to ensure that all system pods are running after the certificate update:

```
# kubectl get pods -A ↵
```

The status of each pod is listed; the NSP cluster is operational when each pod STATUS value is Running or Completed.

10

If the cluster fails to become operational after the typical initialization period, record the cluster status and contact technical support.

11

When the cluster is operational, close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.7 How do I update nsp_kubeconfig on the NSP deployer host?

7.7.1 Purpose

Perform this procedure if SSH access between the NSP deployer host and cluster host is disabled.

Note: You require root user privileges on the NSP deployer VM.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

7.7.2 Steps

1

Open a terminal session to the NSP deployer VM

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

4

Enter the following to resynchronize the kubeconfig files on the NSP cluster:

```
# ./nspk8sctl update --kubeconfig ↵
```

The nsp_kubeconfig files are updated on the deployer host.

END OF STEPS

7.8 How do I add Kubernetes load balancer external IP addresses?

7.8.1 Purpose

Use this procedure to configure additional Kubernetes load balancer external IP addresses after Kubernetes has been installed.

7.8.2 Steps

1

Open a terminal session to the NSP deployer VM.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Log in as the root or NSP admin user.

3

Open the following file using a plain-text editor such as vi:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

4

In the following section, specify virtual IP addresses for NSP to use as external load-balancer endpoints.

```
loadBalancerExternalIps:
- <ext_loadBalancer_IP>
- <ext_loadBalancer_IP>
...
```

5

Save and close the file.

6

Rerun the Kubernetes installer.

```
# cd /opt/nsp/nsp-k8s-deployer-new-release-ID/bin
# ./nspk8sctl install ↵
```

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP cluster TLS administration procedures

7.9 How do I list the NSP Kubernetes secrets?

7.9.1 Purpose

Perform this procedure to list the Kubernetes secrets created using the NSP secret management tool in an NSP cluster.

7.9.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Enter the following:

```
# kubectl get secret -A -l "nspdeployer-secret=true" ↵
```

The secrets are listed, as shown in the following example:

```
NAMESPACE     NAME              TYPE     DATA      AGE
namespace     secret_name       type     num_arts  age
```

where

namespace is the namespace of the secret

secret_name is the displayed name of the secret

type is the secret type

num_arts is the number of TLS file artifacts that the secret contains

age is the number of days since secret creation

4

View the secrets, as required.

5

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.10 How do I view the Kubernetes secret content?

7.10.1 Purpose

Perform this procedure to show a description of each Kubernetes secret in an NSP cluster.

7.10.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

4

Enter the following:

```
# ./nspdeployerctl secret describe ↵
```

The content of each secret is displayed; the following example shows the output for one secret:

```
Secret: secret_name
  secret_description
Namespaces: associated_namespaces
Status: status
Immutable: no
Content:
  tls.key,tls.crt (cert_type CA key pair), type=cacert(days=365),
status=status
  tls.key (cert_type CA private key), type=file, value=<prompted>,
status=status
  tls.crt (cert_type CA certificate), type=file, value=<prompted>,
status=status
```

The *status* reads **active** unless the secret is deleted, in which case the status reads **inactive**.

5

View the secrets, as required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Close the console window.

END OF STEPS

7.11 How do I update the NSP issuer TLS certificates?

7.11.1 Purpose

CAUTION

Potential Service Disruption

Updating the TLS certificates requires that you stop and restart each NSP cluster, which is potentially service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance window under the guidance of technical support.

Perform this procedure to replace the internal or external TLS keys or certificates, as may be required when a certificate nears or reaches expiry, or as required by your company security policy.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

7.11.2 Steps

1

Perform Step 6 to Step 11 in the standalone or primary data center.

2

If the NSP deployment is DR, perform Step 6 to Step 11 in the standby data center.

3

Perform Step 12 to Step 14 in the standalone or primary data center.

4

If the NSP deployment is DR, perform Step 12 to Step 14 in the standby data center.

5

Go to Step 15.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Open a terminal session to the NSP deployer VM.

7

Log in as the root or NSP admin user.

8

Stop the NSP cluster.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
`nspdeployerctl --ask-pass uninstall --undeploy`

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```

3. Save and close the file.
4. Enter the following:

   # **cd /opt/nsp/NSP-CN-DEP-*release-ID*/bin** ↵

5. Enter the following:

   # **./nspdeployerctl uninstall --undeploy** ↵

   The NSP cluster stops.

9

To replace the internal NSP issuer CA certificate/key pair, enter the following:

./nspdeployerctl secret -s ca-key-pair-internal-nspdeployer -n "*" -f tls.key=*key_file* -f tls.crt=*cert_file* update ↵

where

key_file is the full path and name of the TLS key file

cert_file is the full path and name of the TLS certificate file

Messages like the following are displayed:

```
tls.crt=key_file update
secret/ca-key-pair-internal-nspdeployer patched
secret/ca-key-pair-internal-nspdeployer patched
secret/ca-key-pair-internal-nspdeployer patched
The following files may contain sensitive information. They are no
longer required by NSP and may be removed.
  key_file
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
  cert_file
```

10

To replace the external NSP issuer CA certificate/key pair, enter the following:

```
# ./nspdeployerctl secret -s ca-key-pair-external-nspdeployer -n "*"
-f tls.key=key_file -f tls.crt=cert_file update ↵
```

where

key_file is the full path and name of the TLS CA private key file

cert_file is the full path and name of the TLS CA certificate file

Messages like the following are displayed:

```
tls.crt=key_file update
secret/ca-key-pair-external-nspdeployer patched
secret/ca-key-pair-external-nspdeployer patched
secret/ca-key-pair-external-nspdeployer patched
The following files may contain sensitive information. They are no
longer required by NSP and may be removed.
  key_file
  cert_file
```

11

Back up the Kubernetes secrets.

1. Enter the following:

   ```
   # ./nspdeployerctl secret -o backup_file backup ↵
   ```

   where *backup_file* is the full path and name of the backup file to create

   As the secrets are backed up, messages like the following are displayed for each Kubernetes namespace:

   ```
   Backing up secrets to /opt/backupfile...
     Including secret namespace:ca-key-pair-external
     Including secret namespace:ca-key-pair-internal
     Including secret namespace:nsp-tls-store-pass
   ```

   When the backup is complete, the following prompt is displayed:

   ```
   Please provide an encryption password for backup_file
   enter aes-256-ctr encryption password:
   ```

2. Enter a password.

   The following prompt is displayed:

   ```
   Verifying - enter aes-256-ctr encryption password:
   ```

3. Re-enter the password.

   The backup file is encrypted using the password.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4. Record the password for use when restoring the backup.
5. Record the name of the data center associated with the backup.
6. Transfer the backup file to a secure location in a separate facility for safekeeping.

12

Enter the following to start the NSP cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config --deploy

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster starts, and the configuration update is put into effect.

13

To delete the local certificate and key files on an NSP deployer VM, enter the following for each file identified for removal in Step 9 and Step 10:

```
# rm file ↵
```

where *file* is one of the following:

- *cert_file*
- *key_file*

14

Perform the following as required to update the TLS certificates on each NSP component deployed outside the NSP cluster:

- 7.18 “How do I configure an NSP auxiliary database to request the NSP TLS certificate?” (p. 142)
- 7.19 “How do I configure an NFM-P main server to request the NSP TLS certificate?” (p. 143)
- 7.20 “How do I configure an NFM-P auxiliary server to request the NSP TLS certificate?” (p. 146)
- 7.21 “How do I enable TLS for NFM-P XML API clients?” (p. 149)
- 7.22 “How do I disable TLS for NFM-P XML API clients?” (p. 152)

15

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.12 How do I update the custom NSP server TLS certificates?

7.12.1 Purpose

CAUTION

Potential Service Disruption

If you are providing a new CA certificate, you must stop and restart each NSP cluster, which is potentially service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance window under the guidance of technical support.

Perform this procedure to update the custom TLS certificates for NSP client access.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

7.12.2 Steps

1

Log in as the root or NSP admin user on the standalone or primary NSP deployer VM.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

4

If you are providing a new CA certificate, stop the NSP cluster.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
`nspdeployerctl --ask-pass uninstall --undeploy`

1. Open the following file using a plain-text editor such as vi:
   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
deleteOnUndeploy:false
```

3. Save and close the file.
4. Enter the following:

   # cd /opt/nsp/NSP-CN-DEP-*release-ID*/bin ↵
5. Enter the following:

   # ./nspdeployerctl uninstall --undeploy ↵

   The NSP cluster stops.

5

Perform one of the following.

a. If you created secrets without customer certificates during NSP installation, you must create the nginx-nb-tls-nsp secret.

   Enter the following:

   # ./nspdeployerctl secret -s nginx-nb-tls-nsp -n psaRestricted -f tls.key=*customKey* -f tls.crt=*customCert* -f ca.crt=*customCaCert* create ↵

   where

   customKey is the full path of the private server key file

   customCert is the full path of the server public certificate file

   customCaCert is the full path of the CA public certificate file

b. If you are providing a new client certificate and key, but the CA certificate is unchanged, perform the following steps:

   Enter the following:

   # ./nspdeployerctl secret -s nginx-nb-tls-nsp -n psaRestricted -f tls.key=*customKey* -f tls.crt=*customCert* update ↵

   where

   customKey is the full path of the private server key file

   customCert is the full path of the server public certificate file

c. If you are providing a new CA certificate with the new client certificate and key, enter the following:

   # ./nspdeployerctl secret -s nginx-nb-tls-nsp -n psaRestricted -f tls.key=*customKey* -f tls.crt=*customCert* -f ca.crt=*customCaCert* update ↵

   where

   customKey is the full path of the private server key file

   customCert is the full path of the server public certificate file

   customCaCert is the full path of the CA public certificate file

   Messages like the following are displayed as the server secret is updated:

   ```
   secret/nginx-nb-tls-nsp patched
   ```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
The following files may contain sensitive information. They are no
longer required by NSP and may be removed.
  customKey
  customCert
  customCaCert
```

6

If you are providing a new CA certificate that is not in the same location as the previous certificate, update the NSP configuration.

1. Open the following file with a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Configure the following **tls** parameter in the **deployment** section:

   ```
   tls:
     trustedCertificates: certificate_path
   ```

   where *certificate_path* is the full path and name of the CA certificate file

3. Save and close the file.

7

Enter the following to start the NSP cluster:

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster starts, and the configuration update is put into effect.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config --deploy

8

To delete the local certificate and key files on an NSP deployer VM, enter the following for each file identified for removal in Step 5:

```
# rm file ↵
```

where *file* is one of the following:

- *cert_file*
- *key_file*
- *CA_cert_file*

9

Configure each other NSP component to obtain the updated TLS configuration.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10

Close the open console window.

END OF STEPS

7.13 How do I add an NSP Kubernetes secret?

7.13.1 Purpose

Perform this procedure to add a new Kubernetes secret to an NSP cluster, for example, when a new type of interface is added to the cluster.

Note: You must perform the procedure on each NSP cluster in a DR deployment.

7.13.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

4

Enter the following:

Note: The help option lists all command options:
`./nspdeployerctl secret help`

Note: The describe option lists all secrets and the contained parameters:
`./nspdeployerctl secret describe`

```
# ./nspdeployerctl secret -s newsecret -n namespace -v parameter=value
create ↵
```

where

newsecret is the new secret name, which can include only:

- lowercase alphanumeric characters
- hyphen
- period

namespace is the name of the restricted Kubernetes namespace

parameter is the name of the parameter to set in the secret

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

value is the parameter value to set

The *newsecret* secret is created, and the following message is displayed:

```
secret/newsecret created
```

The secret holds a private key and a public key.

5

Enter the following to back up all Kubernetes secrets:

1. Enter the following:

   ```
   # ./nspdeployerctl secret -o backup_file backup ↵
   ```

   where *backup_file* is the full path and name of the backup file to create

   As the secrets are backed up, messages like the following are displayed for each Kubernetes namespace:

   ```
   Backing up secrets to /opt/backupfile...
     Including secret namespace:ca-key-pair-external
     Including secret namespace:ca-key-pair-internal
     Including secret namespace:nsp-tls-store-pass
   ```

   When the backup is complete, the following prompt is displayed:

   ```
   Please provide an encryption password for backup_file
   enter aes-256-ctr encryption password:
   ```

2. Enter a password.

   The following prompt is displayed:

   ```
   Verifying - enter aes-256-ctr encryption password:
   ```

3. Re-enter the password.

   The backup file is encrypted using the password.

4. Record the password for use when restoring the backup.
5. Record the name of the data center associated with the backup.
6. Transfer the backup file to a secure location in a separate facility for safekeeping.

6

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.14 How do I recreate the NSP Kubernetes secrets?

7.14.1 Purpose



CAUTION

Potential Service Disruption

Recreating the NSP Kubernetes secrets requires a shutdown and restart of each NSP cluster, which is service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance window under the guidance of technical support.

The following scenarios require the recreation of the Kubernetes secrets in an NSP cluster:

- After a catastrophic NSP cluster failure
- After a Kubernetes uninstallation, which removes the secrets, in the event that you need to reinstall Kubernetes

Perform the procedure on each NSP cluster that requires recreated secrets.

7.14.2 Steps

1

Open a terminal session to the NSP deployer VM

2

Log in as the root or NSP admin user.

3

Stop the NSP cluster.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
`nspdeployerctl --ask-pass uninstall --undeploy`

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```

3. Save and close the file.
4. Enter the following:

   `# cd /opt/nsp/NSP-CN-DEP-release-ID/bin` ↵

5. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ./nspdeployerctl uninstall --undeploy ↵
```

The NSP cluster stops.

4

Enter the following to uninstall the current secrets:

```
# ./nspdeployerctl secret uninstall ↵
```

Messages like the following are displayed as each secret is uninstalled.

```
Removing secret secret...
  Removing from namespace nsp-psa-baseline
secret "secret" deleted
  Removing from namespace nsp-psa-privileged
secret "secret" deleted
  Removing from namespace nsp-psa-restricted
secret "secret" deleted
```

5

Enter the following:

```
# ./nspdeployerctl secret install ↵
```

The following prompt is displayed:

```
Would you like to use your own CA key pair for the NSP Internal
Issuer? [yes,no]
```

6

Perform one of the following.

a. Enter no ↵.

   The NSP generates the internal key and certificate files.

b. Provide your own certificate to secure the internal network.

   1. Enter yes ↵.

      The following messages and prompt are displayed:

   2. ```
      Building secret 'ca-key-pair-internal-nspdeployer'
      The CA key pair used to sign certificates generated by the NSP
      Internal Issuer.
      Please enter the internal CA private key:
      ```

   3. Enter the full path of the internal private key.

      The following prompt is displayed:

      ```
      Please enter the internal CA certificate:
      ```

   4. Enter the full path of the internal certificate:

      The following messages are displayed for each Kubernetes namespace:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms
      ```

```
Adding secret ca-key-pair-internal-nspdeployer to namespace
namespace...
secret/ca-key-pair-internal-nspdeployer created
```

The following prompt is displayed:

```
Would you like to use your own CA key pair for the NSP External
Issuer? [yes,no]
```

7

Perform one of the following.

a. Enter no ↵.

The NSP generates the external key and certificate files.

b. Provide your own certificate to secure the external network.

1. Enter yes ↵.

The following messages and prompt are displayed:

```
Building secret 'ca-key-pair-external-nspdeployer'
The CA key pair used to sign certificates generated by the NSP
External Issuer.
Please enter the external CA private key:
```

2. Enter the full path of the external private key.

The following prompt is displayed:

```
Please enter the external CA certificate:
```

3. Enter the full path of the external certificate:

The following messages are displayed for each Kubernetes namespace:

```
Adding secret ca-key-pair-external-nspdeployer to namespace
namespace...
secret/ca-key-pair-external-nspdeployer created
```

```
Would you like to provide a custom private key and certificate for use
by NSP endpoints when securing TLS connections over the client
network? [yes,no]
```

8

Perform one of the following.

a. Enter no ↵.

The NSP generates the client key and certificate files.

b. Provide your own certificate for the client network.

1. Enter yes ↵

The following messages and prompt are displayed:

```
Building secret 'nginx-nb-tls-nsp'
TLS certificate for securing the ingress gateway.
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Please enter the ingress gateway private key:
```

2. Enter the full path of the private key file for client access.

   The following prompt is displayed:

   ```
   Please enter the ingress gateway public certificate:
   ```

3. Enter the full path of the public certificate file for client access.

   The following prompt is displayed:

   ```
   Please enter the ingress gateway public trusted CA certificate
   bundle:
   ```

4. Enter the full path of the public trusted CA certificate bundle file.

   The following message is displayed:

   ```
   Adding secret nginx-nb-tls-nsp to namespace namespace...
   ```

9

If the deployment includes MDM, the following prompt is displayed:

```
Would you like to provide mTLS certificates for the NSP mediation
interface for two-way TLS authentication? [yes,no]
```

Perform one of the following.

a. Enter no ↵ if you are not using mTLS or have no certificate to provide for mTLS.

b. Provide your own certificate to secure MDM and gNMI telemetry.

   1. Enter yes ↵.
   2. The following messages and prompt are displayed:

      ```
      Building secret 'mediation-mtls-key'
      mTLS artifacts use to secure MDM communications with nodes.
      Please enter the mediation private key:
      ```

   3. Enter the full path of the mediation private key.

      The following prompt is displayed:

      ```
      Please enter the mediation CA certificate:
      ```

   4. Enter the full path of the mediation CA certificate.

      The following messages are displayed:

      ```
        Adding secret mediation-mtls-key to namespace namespace...
      secret/mediation-mtls-key created
        Adding secret mediation-mtls-key to namespace namespace...
      secret/mediation-mtls-key created
      ```

10

Back up the secrets.

1. Enter the following:

   ```
   # ./nspdeployerctl secret -o backup_file backup ↵
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

where *backup_file* is the full path and name of the backup file to create

As the secrets are backed up, messages like the following are displayed for each Kubernetes namespace:

```
Backing up secrets to /opt/backupfile...
  Including secret namespace:ca-key-pair-external
  Including secret namespace:ca-key-pair-internal
  Including secret namespace:nsp-tls-store-pass
```

When the backup is complete, the following prompt is displayed:

```
Please provide an encryption password for backup_file
enter aes-256-ctr encryption password:
```

2. Enter a password.

   The following prompt is displayed:

   ```
   Verifying - enter aes-256-ctr encryption password:
   ```

3. Re-enter the password.

   The backup file is encrypted using the password.

4. Record the password for use when restoring the backup.
5. Record the name of the data center associated with the backup.
6. Transfer the backup file to a secure location in a separate facility for safekeeping.

11

If the NSP is a DR deployment, obtain and restore the NSP secrets backup file from the NSP cluster in the primary data center.

1. Enter the following on the standby NSP deployer VM:

   # scp *address*:*path/backup_file* /tmp/ ↵

   where

   address is the address of the NSP deployer VM in the primary cluster

   path is the full path of the backup file created in Step 10

   backup_file is the secrets backup file name

   The backup file is transferred to the local /tmp directory.

2. Enter the following:

   # cd /opt/nsp/NSP-CN-DEP-*release-ID*/bin ↵

3. Enter the following:

   ./nspdeployerctl secret -i /tmp/*backup_file* restore ↵

   The following prompt is displayed:

   ```
   Please provide the encryption password for /opt/backupfile
   enter aes-256-ctr decryption password:
   ```

4. Enter the password recorded in Step 10.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

As the secrets are restored, messages like the following are displayed for each Kubernetes namespace:

```
Restoring secrets from backup_file...
secret/ca-key-pair-external created
  Restored secret namespace:ca-key-pair-external
secret/ca-key-pair-internal created
  Restored secret namespace:ca-key-pair-internal
secret/nsp-tls-store-pass created
  Restored secret namespace:nsp-tls-store-pass
```

5. If you answer yes to the Step 8 prompt for client access during the primary NSP cluster configuration, you must update the standby server secret for client access using the custom certificate and key files that are specific to the standby cluster.

   Enter the following:

   ```
   # ./nspdeployerctl secret -s nginx-nb-tls-nsp -n psaRestricted -f
   tls.key=customKey -f tls.crt=customCert -f ca.crt=customCaCert
   update ↲
   ```

   where

   customKey is the full path of the private server key file

   customCert is the full path of the server public certificate file

   customCaCert is the full path of the CA public certificate file

   Messages like the following are displayed as the server secret is updated:

   ```
   secret/nginx-nb-tls-nsp patched
   The following files may contain sensitive information. They are no
   longer required by NSP and may be removed.
     customKey
     customCert
     customCaCert
   ```

12

Enter the following to start the NSP cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config --deploy

```
# ./nspdeployerctl install --config --deploy ↲
```

The NSP cluster starts, and the configuration update is put into effect.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13

Close the console window.

END OF STEPS

7.15 How do I back up the NSP Kubernetes secrets?

7.15.1 Steps

Perform the following steps in each data center to back up the Kubernetes secrets.

1

Open a terminal session to the NSP deployer VM and log in as the root or NSP admin user.

2

Enter the following on the NSP deployer VM:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

3

Enter the following:

```
# ./nspdeployerctl secret -o backup_file backup ↵
```

where *backup_file* is the absolute path and name of the backup file to create

As the secrets are backed up, messages like the following are displayed for each Kubernetes namespace:

```
Backing up secrets to /opt/backupfile...
  Including secret namespace:ca-key-pair-external
  Including secret namespace:ca-key-pair-internal
  Including secret namespace:nsp-tls-store-pass
```

When the backup is complete, the following prompt is displayed:

```
Please provide an encryption password for backup_file
enter aes-256-ctr encryption password:
```

4

Enter a password.

The following prompt is displayed:

```
Verifying - enter aes-256-ctr encryption password:
```

5

Re-enter the password.

The backup file is encrypted using the password.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Record the password for use when restoring the backup.

7

Record the name of the data center associated with the backup.

8

Copy *backup_file* to a backup directory.

END OF STEPS

7.16 How do I restore the NSP Kubernetes secrets?

7.16.1 Steps

Note: Ensure that you restore each backup file on the correct NSP cluster; an NSP secrets backup is specific to an NSP cluster.

Perform the following steps in each data center to restore the NSP Kubernetes secrets.

1

Open a terminal session to the NSP deployer VM and log in as the root or NSP admin user.

2

Enter the following on the NSP deployer VM:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

3

Enter the following:

```
./nspdeployerctl secret -i backup_file restore ↵
```

where *backup_file* is the absolute path and filename of the secrets backup file to restore

The following prompt is displayed:

```
Please provide the encryption password for /opt/backupfile
enter aes-256-ctr decryption password:
```

4

Enter the password recorded during the backup creation.

As the secrets are restored, messages like the following are displayed for each Kubernetes namespace:

```
Restoring secrets from backup_file...
secret/ca-key-pair-external created
  Restored secret namespace:ca-key-pair-external
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
secret/ca-key-pair-internal created
  Restored secret namespace:ca-key-pair-internal
secret/nsp-tls-store-pass created
  Restored secret namespace:nsp-tls-store-pass
```

END OF STEPS

7.17 How do I update the Keycloak OpenSearch client secret?

7.17.1 Purpose



CAUTION

Potential Service Disruption

Updating the OpenSearch Keycloak secret requires a shutdown and restart of the Keycloak pod, which is service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance window under the guidance of technical support.

Perform this procedure to update the Keycloak OpenSearch client secret on either a standalone NSP deployment or a DR deployment.

7.17.2 Steps

1

Open a terminal session to the NSP deployer VM and log in as the root or NSP admin user.

2

On the active deployer VM, update the keycloak-opensearch-client user name (OpenSearch Client ID) to the desired new ID value:

```
# <deployer dir>/nspdeployerctl secret -n nsp-psa-restricted -s
keycloak-opensearch-client -v keycloak-opensearch-client=<new_id>
update
```

3

(Optional) If the secret value also needs to be updated, on the active deployer VM, update the keycloak-opensearch-client secret (Opensearch Client Secret) to the desired new secret value:

```
# <deployer dir>/nspdeployerctl secret -n nsp-psa-restricted -s
keycloak-opensearch-client -v keycloak-opensearch-client-secret=<new_
secret> update
```

4

Restart the Keycloak pod.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

If this update is on a DR deployment, backup the updated keycloak-opensearch-client secret to a file and copy it to the standby deployer VM. On the active deployer VM:

```
# <deployer dir>/nspdeployerctl secret -n nsp-psa-restricted -s
keycloak-opensearch-client -o keycloak-opensearch-client.aes fetch
```

6

Copy over the keycloak-opensearch-client.aes file from the active deployer VM to the standby deployer VM.

7

Open a terminal session to the standby deployer VM and log in as the root or NSP admin user.

8

On the standby deployer VM, update the keycloak-opensearch-client secret:

```
# <deployer dir>/nspdeployerctl secret -n nsp-psa-restricted -s
keycloak-opensearch-client -f keycloak-opensearch-client.aes update
```

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP component TLS configuration

7.18 How do I configure an NSP auxiliary database to request the NSP TLS certificate?

7.18.1 Purpose

The following steps describe how to configure an NSP auxiliary database to request a TLS certificate from the NSP cluster, as is required when a new or updated certificate is available.

7.18.2 Steps

1

Log in as the root user on an auxiliary database station.

2

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

3

Enter the following to regenerate the TLS certificates:

```
# ./auxdbAdmin.sh configureTLS ↵
```

4

Enter the following to restart the auxiliary database services:

```
# ./auxdbAdmin.sh stopAndDisableServices ↵
# ./auxdbAdmin.sh startAndEnableServices ↵
```

Note: If the auxiliary database is geo-redundant, you must perform these steps on a station in each auxiliary database cluster.

5

Close the open console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.19 How do I configure an NFM-P main server to request the NSP TLS certificate?

7.19.1 Purpose

CAUTION

Service Disruption

Performing the procedure requires that you shut down the main server, which may be service-affecting.

If the main server is in service, ensure that you perform the procedure only during a scheduled maintenance period.

The following steps describe how to configure an NFM-P main server to request a TLS certificate from the NSP cluster, as required when a new or updated certificate is available.

7.19.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Stop the main server.

1. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

2. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The main server is stopped when the following message is displayed:

   ```
   Main Server is stopped
   ```

   If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status.

   Do not proceed to the next step until the server is completely stopped.

4. Enter the following to switch to the root user:

   ```
   bash$ su ↲
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Enter the following:

```
# samconfig -m main ↲
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

5

Enter the following:

```
<main> configure tls ↲
```

The prompt changes to `<main configure tls>`.

6

Enter the following:

```
<main configure tls> regenerate-certs ↲
```

7

Enter the following:

```
<main configure tls> no keystore-file ↲
```

8

Enter the following:

```
<main configure tls> no truststore-file ↲
```

9

Perform one of the following:

a. Enter the following to use the default keystore password, which is available from technical support:

```
<main configure tls> no keystore-pass ↲
```

b. Enter the following to assign a keystore password:

```
<main configure tls> keystore-pass password ↲
```

where *password* is the password to assign

10

Perform one of the following:

a. Enter the following to use the default truststore password, which is available from technical support:

```
<main configure tls> no truststore-pass ↲
```

b. Enter the following to assign a truststore password:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
<main configure tls> truststore-pass password ↵
```

where *password* is the password to assign

11

Enter the following:

```
<main configure tls> alias alias ↵
```

where *alias* is the keystore alias to assign

12

Enter the following:

```
<main configure tls> pki-server address ↵
```

where *address* is one of the following values in the **platform**—**ingressApplications**—**ingressController** section of the config.yml file on the local NSP deployer VM:

In the **internalAddresses** subsection, if configured, otherwise, in the **clientAddresses** subsection:

- if configured, the **advertised** value
- otherwise, the **virtualIp** value

13

Enter the following:

```
<main configure tls> pki-server-port 80 ↵
```

14

Enter the following:

```
<main configure tls> exit ↵
```

The prompt changes to `<main>`.

15

Enter the following:

```
<main> apply ↵
```

The configuration is applied.

The main server:

- generates a TLS certificate
- sends a CSR to the PKI server
- receives from the PKI server the signed TLS certificate

16

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
<main> exit ↲
```

The samconfig utility closes.

17

Enter the following to return to the nsp user:

```
# exit ↲
```

18

Start the main server.

1. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↲
   ```

2. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

19

Close the console window.

END OF STEPS

7.20 How do I configure an NFM-P auxiliary server to request the NSP TLS certificate?

7.20.1 Purpose

CAUTION

Service Disruption

Performing the procedure requires that you shut down the auxiliary server, which may be service-affecting.

If the auxiliary server is in service, ensure that you perform the procedure only during a scheduled maintenance period.

The following steps describe how to configure an NFM-P auxiliary server to request a TLS certificate from the NSP cluster, as is required when a new or updated certificate is available.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7.20.2 Steps

1

Log in to the auxiliary server station as the nsp user.

2

Open a console window.

3

Stop the auxiliary server.

1. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/auxserver/nms/bin ↲
   ```

2. Enter the following:

   ```
   bash$ ./auxnmsserver.bash auxstop ↲
   ```

3. Enter the following:

   ```
   bash$ ./auxnmsserver.bash auxappserver_status ↲
   ```

   The auxiliary server is stopped when the following message is displayed:

   ```
   Auxiliary Server is stopped
   ```

   If the command output indicates that the server is not completely stopped, wait five minutes and then re-enter the command in this step to check the server status.

   Do not proceed to the next step until the server is completely stopped.

4

Enter the following to switch to the root user:

```
bash$ su - ↲
```

5

Enter the following:

```
# samconfig -m aux ↲
```

The following is displayed:

```
Start processing command line inputs...
<aux>
```

6

Enter the following:

```
<aux> configure tls ↲
```

The prompt changes to `<aux configure tls>`.

7

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
<aux configure tls> no keystore-file ↲
```

8

Perform one of the following:

a. Enter the following to use the default keystore password, which is available from technical support:

```
<aux configure tls> no keystore-pass ↲
```

b. Enter the following to assign a keystore password:

```
<aux configure tls> keystore-pass password ↲
```

where *password* is the password to assign

9

Enter the following:

```
<main configure tls> pki-server address ↲
```

where *address* is one of the following values in the **platform**—**ingressApplications**—**ingressController** section of the config.yml file on the local NSP deployer VM:

In the **internalAddresses** subsection, if configured, otherwise, in the **clientAddresses** subsection:

- if configured, the **advertised** value
- otherwise, the **virtualIp** value

10

Enter the following:

```
<main configure tls> pki-server-port 80 ↲
```

11

Enter the following:

```
<aux configure tls> exit ↲
```

The prompt changes to `<aux>`.

12

Enter the following:

```
<aux> apply ↲
```

The configuration is applied.

The auxiliary server:

- generates a TLS certificate
- sends a CSR to the PKI server
- receives from the PKI server the signed TLS certificate

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13

Enter the following:

```
<aux> exit ↲
```

The samconfig utility closes.

14

Enter the following to return to the nsp user:

```
# exit ↲
```

15

Start the auxiliary server.

1. Enter the following:

   ```
   bash$ ./auxnmsserver.bash auxstart ↲
   ```

2. Enter the following:

   ```
   bash$ ./auxnmsserver.bash auxappserver_status ↲
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Auxiliary Server process is running.  See auxnms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

16

Close the console window.

END OF STEPS

7.21 How do I enable TLS for NFM-P XML API clients?

7.21.1 Purpose

The following steps describe how to enable TLS for all XML API client communication with the NFM-P.

CAUTION

Service Disruption

Performing the procedure involves stopping and starting each main server, which is service-affecting.

You must perform the procedure only during a scheduled maintenance window.

Note: You require the following user privileges on the main server station:

- root

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- nsp

Note: The Bash shell is the supported command shell for RHEL CLI operations.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

7.21.2 Steps

1

Perform the following on each main server station to stop the main server.

Note: In a redundant system, you must stop the standby main server first.

1. Log in to the main server station as the nsp user.
2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

5. Enter the following to switch to the root user:

   ```
   bash$ su ↵
   ```

2

When the main servers are stopped, perform the following on each main server station.

1. Enter the following:

   ```
   # samconfig -m main ↵
   ```

   The following is displayed:

   ```
   Start processing command line inputs...
   <main>
   ```

2. Enter the following:

   ```
   <main> configure oss secure back ↵
   ```

   The prompt changes to `<main configure>`.

3. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
<main configure> back ↲
```

The prompt changes to `<main>`.

4. Enter the following:

```
<main> apply ↲
```

The configuration is applied.

5. Enter the following:

```
<main> exit ↲
```

The samconfig utility closes.

3

Perform the following on each main server station to start the main server.

Note: In a redundant system, you must start the primary main server first.

1. Enter the following to switch back to the nsp user:

```
# exit ↲
```

2. Enter the following:

```
bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
```

3. Enter the following:

```
bash$ ./nmsserver.bash start ↲
```

4. Enter the following:

```
bash$ ./nmsserver.bash appserver_status ↲
```

The server status is displayed; the server is fully initialized if the status is the following:

```
Application Server process is running.  See nms_status for more
detail.
```

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

4

Perform the following steps on each XML API client station.

1. If you deployed TLS using a PKI server, perform one of the following.
   a. Transfer the ca.pem certificate file from the PKI server station to the OSS client station.
   b. Use the PKI server REST API to obtain the certificate; see the online NSP REST API documentation for information.
2. If you deployed TLS using the manual method, transfer your certificate file to the OSS client station.
3. Import the TLS certificate from the certificate file to the TLS certificate store of the client station OS; see the OS documentation for information about importing a certificate.
4. Modify each main server XML API URL on the OSS client station:
   - Change http: to https:.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Change the URL port value from 8080 to 8443.

END OF STEPS

7.22 How do I disable TLS for NFM-P XML API clients?

7.22.1 Purpose

The following steps describe how to disable TLS for all XML API clients in order to support OSS clients in a non-secure environment.

Note: Disabling TLS on the XML API also disables TLS for all clients that use the XML API, and for NFM-P GUI clients. Browser-based clients are unaffected, and must use HTTPS for access.

Note: Disabling TLS on the NFM-P XML API does not disable the NFM-P REST API.

CAUTION

Service Disruption

Performing the procedure involves stopping and starting each main server, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period of low network activity.

Note: You require the following user privileges on the main server station:

- root
- nsp

Note: The Bash shell is the supported command shell for RHEL CLI operations.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

7.22.2 Steps

1

Perform the following steps on each main server station to stop the main server.

Note: In a redundant system, you must stop the standby main server first.

1. Log in to the main server station as the nsp user.
2. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
```

3. Enter the following:

```
bash$ ./nmsserver.bash stop ↲
```

4. Enter the following:

```
bash$ ./nmsserver.bash appserver_status ↲
```

The server status is displayed; the server is fully stopped if the status is the following:

```
Application Server is stopped
```

If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

5. Enter the following to switch to the root user:

```
bash$ su ↲
```

2

When the main servers are stopped, perform the following on each main server station.

1. Enter the following:

```
# samconfig -m main ↲
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

2. Enter the following:

```
<main> configure oss no secure back ↲
```

The prompt changes to `<main configure>`.

3. Enter the following:

```
<main configure> back ↲
```

The prompt changes to `<main>`.

4. Enter the following:

```
<main> apply ↲
```

The configuration is applied.

5. Enter the following:

```
<main> exit ↲
```

The samconfig utility closes.

3

Perform the following on each main server station to start the main server.

Note: In a redundant system, you must start the primary main server first.

1. Enter the following to switch back to the nsp user:

```
# exit ↲
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↵
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

4

Close the console window.

5

On each XML API client station, modify the URL that the client uses to reach the main server.

1. Change https: to http:.
2. Change the URL port value from 8443 to 8080.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8 NSP user security

User management

8.1 What is user management?

8.1.1 Local user management

NSP has a local user database that supports locally defined users with OAUTH2 user authentication. NSP can also work with remote LDAP, RADIUS, and TACACS authentication agents. If NSP is integrated with NFM-P, you can import your NFM-P users into the NSP local user database.

For all local and remote users, the Users and System Security GUI lists information that includes the authentication source, the user creation time, and the most recent login time.

Note: The NSP does not support case-sensitive user names; local and remote user names are saved in lowercase. User name entry at sign-in is case-insensitive.

NSP Users and Security supports up to 5000 users, except where noted.

Nokia does not support direct customer access to the Keycloak admin console.

8.1.2 Remote user management

NSP supports remote LDAP (including Active Directory), RADIUS, and TACACS authentication servers.

With remote user management, the NSP first attempts to verify login attempts against the local user database. If the user account is not found locally, NSP searches the remote authentication servers (LDAP first, followed by RADIUS or TACACS). If a user account is found in an authentication source (local or remote) but fails the password check, the authentication attempt stops and does not continue to any other authentication sources.

Note: NSP Users and Security supports a maximum combined total of 1000 local and remote users when Active Directory is configured.

Remote login attempts can be handled in the following ways, with regards to user group assignment:

- If a remote user attempts to log into NSP and the remote authentication source does not specify a user group for the remote user, then the user is assigned to the NSP default user group and will have access in accordance with the roles assigned to the default user group.
- If a remote user attempts to log into NSP and the remote authentication source does not specify a user group for the remote user, and NSP does not have a default user group configured, then the remote user login to NSP is denied.
- If a remote user attempts to log into NSP and the remote authentication source specifies a user group for the remote user, but that user group is not configured in NSP, then the remote user login to NSP is denied.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

LDAP/AD user auto-import behavior in NSP

If NSP is configured for remote user authentication with an LDAP or Active Directory server, eligible LDAP/AD users automatically import into NSP and appear as local accounts in the NSP database.

Auto-import of LDAP or AD users depends on:

- the objectClass attributes assigned to users in the LDAP/AD server
- the userObjectClasses filter defined in NSP's LDAP/AD configuration

Examples:

- If userObjectClasses is set to "person,organizationalPerson,user" in NSP, only LDAP/AD users whose objectClass includes all three values are auto-imported.
- If userObjectClasses is set to "person" only, then any LDAP/AD user whose objectClass list includes "person" is auto-imported into NSP.
- Users that do not meet the userObjectClasses filter criteria described in the above two examples are not auto-imported to NSP. However, if such users successfully authenticate through the NSP login, they are imported to NSP at that time.

8.2 What are the NSP user management requirements and restrictions?

8.2.1 Remote users in NSP

Remote users have a local account instance created in the NSP database. Remote users appear in Users and System Security, Users list, flagged with the remote authentication source. Remote users continue to use their login credentials, as defined on the remote server. System administrators can edit certain fields of a remote user local account instance, including first and last name, description and email address; see 8.3 "How do I configure an NSP user?" (p. 159). Remote users are subject to the same global user session limits as locally defined NSP users.

Active Directory

If NSP is configured for remote user authentication with an Active Directory server, the AD users also appear as local accounts in the NSP database. However, AD users are bulk-imported to NSP at system startup. The bulk import of AD users into NSP is automatic and cannot be avoided, but you can manage the scope of the import by defining remote NSP users with a unique distinguished name or user filter, and limiting the user search to that DN only, rather than the subtree.

LDAP, RADIUS, and TACACS

As LDAP, RADIUS, and TACACS users log in to NSP, local account instances are created in the NSP database. Only the remote users that have logged into NSP appear in Users and System Security.

Identity providers

NSP supports Single sign-on (SSO) for NSP users via identity providers (IDPs) that comply with the SAML 2.0 or OpenID Connect standards supported by KeyCloak. The IDP login process may include multi-factor authentication, account verification, and password management policies which

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

are not controlled by any NSP user management settings. IDP users accessing NSP are subject to session management restrictions such as inactivity timeouts and max sessions.

As IDP users successfully log in to NSP, local account instances are created in the NSP database.

The IDP provides a separate user login interface to grant user access to NSP. The NSP login page is configured with redirect links to one or more IDPs. Users enter their login credentials through the IDP and are then redirected to the NSP GUI. NSP also supports OpenID Connect user access to the NSP OSS with a foreign access token.

The following limitations apply to OpenID Connect OSS users:

- Enforcement of maximum OSS sessions is supported.
- Use of the NSP default user group is supported for OpenID Connect accounts with no user group (assuming that a default user group is configured in NSP).
- Access control with RBAC permissions is supported for APIs.

8.2.2 Using multiple remote authentication sources

NSP supports a maximum of 10 remote authentication servers, regardless of the server types in use. This limit includes redundant LDAP servers.

Consider the following information when working with multiple remote authentication sources.

LDAP (including Active Directory)

You can configure multiple LDAP servers in different ways:

- a single LDAP server instance with multiple redundant servers listed.
- multiple LDAP server instances, each with a unique Priority level.
- a combination of both of these arrangements; for example, multiple LDAP server instances, each with unique Priority levels and each with multiple redundant servers.

Be aware of the following restrictions and limitations:

- each secure LDAP/AD server in a redundant configuration requires a TLS certificate.
- the LDAP/AD server IP address/host name/FQDN that is used in the NSP configuration must be in the SAN field of the certificate.
- certificate files must be in PEM format.
- User accounts on LDAP/AD servers should only be duplicated across those servers when they are configured as redundant. When configuring multiple LDAP/AD servers in a prioritized list (where each LDAP/AD server has a different priority), user accounts should not be duplicated across those servers. Local user account instances are associated only with the highest-priority authentication source they exist on.
- When an LDAP/AD server is configured as unavailable or is unreachable by NSP, all local user instances for that source are suspended and unable to login to NSP. Users on other LDAP/AD auth sources will still be able to login. For a redundant LDAP/AD server configuration, those local user account instances will only be suspended when the source is configured unavailable, or all redundant LDAP/AD servers in that configuration are unreachable.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: In an NSP deployment that uses Keycloak with multiple LDAP servers, if the highest-priority LDAP server goes down, users on the second LDAP server will only be able to login to NSP if they already have a local account instance created in the Keycloak database. Otherwise, their login attempts will fail. As a workaround for this scenario, an administrator can disable the operationally-down LDAP server as an authentication source. Then, users on the second LDAP server can login, even if they do not have a local account instance.

RADIUS and TACACS

- Multiple RADIUS *or* TACACS servers are supported. The address field supports multiple comma-separated address:port entries. Each server entry requires a shared secret. The secret field is a comma separated list, and the number of entries must match the numbers of servers in address field. The secret for any server must not contain a comma character.
- The RADIUS server port must be for RADIUS authentication and authorization (default port 1812). The RADIUS accounting port (default port 1813) is not supported.
- Only RADIUS *or* TACACS servers can be configured in a multi-server configuration; not RADIUS *and* TACACS.
- A RADIUS/TACACS multi-server configuration can be enabled or disabled, but not individual servers in a configuration.
- If a RADIUS/TACACS configuration is disabled, all local users associated with the server configuraton are suspended and unavailable for login to NSP.
- In a multi-server configuration, if the first server is unreachable, the second server is used, and so on.
- A user account can be duplicated across multiple servers, but it must have the same user group assignment on each server.
- If a user fails authentication against a RADIUS server, the login attempt is complete and no further RADIUS servers in the multi-server configuration are attempted.
- If a RADIUS server is not reachable when a user is trying to login, Keycloak advances to the next RADIUS server in the configuration and attempt authentication again.
- When a user fails authentication against a TACACS server, Keycloak advances to the next TACACS server in the configuration and attempt authentication again.
- When using multiple RADIUS or TACACS servers, the servers do not need to have identical user information, but any duplicated users must have the same password and usergroup assignment.

8.2.3 E-mail verification

After you enable the Verify Email setting, each local and remote NSP user with a configured e-mail address—not just new users—must complete a verification process. During a subsequent login attempt, the sign-in page directs the operator to open a verification e-mail and click on the enclosed link to complete the process.

After the verification, the user account is tagged as ‘email verified’, and no further verification is required, even if the e-mail address changes.

Note: In order to acquire an API access token, an OSS user that has an e-mail address must first complete the e-mail verification process by signing in to the NSP UI.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.2.4 Forgotten passwords

The NSP sign-in page has a Forgot Password option. If a user clicks this option, they are prompted for their username. A message "You should receive an e-mail shortly ..." appears on the sign-in page. In order to ensure that the Forgot Password option works for local users, configure all local user accounts with e-mail addresses. The Forgot Password feature functions only for local NSP users; remote users cannot reset a password through NSP.

8.2.5 User account lockout messaging

NSP provides the ability to automatically send an e-mail message to users whose accounts have been locked. A user receives an e-mail when they are temporarily or permanently locked out through Brute Force Detection protection mechanisms. Local user accounts must be configured with an e-mail address to be sent lockout messages.

The lockout e-mail function is enabled through the NSP system settings; see 2.8 “How do I configure an e-mail server for notifications?” (p. 41). You can specify the Subject line and body text for the e-mail message.

User account lockout is enforced by Keycloak Brute Force Detection functionality. If account notification is enabled for user lockout and BFD is enabled for temporary or permanent lockout, then the e-mail message to the user account is only triggered on the X+1 bad login attempt, where X is the number of bad login attempts that suspends the user account.

Example:

- User account notification is enabled for user lockout.
- BFD is configured for permanent lockout with maximum bad logins = 3.
- User is configured with an e-mail address.
- User attempts three consecutive bad logins. The account is suspended after the third bad login attempt but the e-mail message to the user is not yet sent.
- User attempts a fourth login. Keycloak sends the e-mail message to the user, notifying them that their account is locked.

Note: Lockout messages are not sent to users whose accounts have been set to Suspended status by an administrator. That is a separate function.

8.2.6 User account login protection

NSP provides functions for temporarily or permanently locking out users for login failures. This includes managing repeated failed login attempts, such as in brute force attacks; see 8.8 “How do I set login protection restrictions?” (p. 168). Temporary lockout protection is configured by default.

8.3 How do I configure an NSP user?

8.3.1 Purpose

This procedure describes how to create or modify NSP user accounts:

- local user accounts that exist only on the NSP database

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP supports up to 5000 local users.

- remote user accounts that correspond to users on remote authentication sources (LDAP, RADIUS, or TACACS).

  NSP configures remote user accounts automatically when they first login to NSP, so there is typically no need to create a remote user account.

You can modify all aspects of a local user account, except for the user name. You can also change a user's password or compel the user to change their password.

You can modify select parameters on remote user accounts. You cannot change the user name or password on a remote user account, nor can you compel a password change.

8.3.2 Steps

1

Open Users and System Security.

2

Select **Users** from the drop-down list on the toolbar.

3

Do one of the following:

a. Click **+Create user**.

b. In the Users list, select a user account you want to modify.

On the user account item, click **⋮Table row actions**, **Edit user**.

4

In the Create|Edit user form, specify user identification information for the account in the Identification section. The **Username** and **User group** fields are mandatory.

Note: Any uppercase characters in the username are saved as lowercase.

The **Username** value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- must **not** include the following special characters: `% + , / : ; = ? [ ] \ " < > # { }`

5

Set the **Account state** for the user to **Active|Suspended**.

6

Select a user group for the user from the **User group** drop-down list.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If no user groups are available, you will need to create one; see 8.20 “How do I configure a user group?” (p. 188).

7

Specify an **Email address** for the account.

8

In the Session configuration section, you can set user account-specific override values for the maximum number of simultaneous NSP GUI sessions and OSS sessions. The override values replace the global maximum sessions settings configured in the NSP Users and Security Settings. By default, all user accounts follow the global max sessions limits.

- To override global GUI session limits, enable the **Override global GUI max sessions** check box and specify the override value in the **User max GUI sessions** field. A zero value means no GUI access for the user.
- To override global OSS session limits, enable the **Override global OSS max sessions** check box and specify the override value in the **User max OSS sessions** field. A zero value means no OSS access for the user.

9

In the Password section, specify and confirm a password for the user account.

Note: The NSP does not support case-sensitive user names; local and remote user names are saved in lowercase. User name entry at sign-in is case-insensitive.

- If you want this password to be temporary, enable the **Force user to change password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the **Show password** option to see the password characters as you type them.
- Click on the **Password requirements** link to view a list of minimum security requirements for the password.

10

Click **Create**.

11

In an NSP deployment that includes the NFM-P, the NFM-P requires a user group with the same name as the NSP user group; otherwise, the NSP user cannot:

- Open an NFM-P client.
- View NSP GUI alarms that quote NFM-P as the source.
- Open some NSP GUI fault-management views.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If your NSP deployment includes the NFM-P, and the NFM-P does not have a user group with the same name as the NSP user group, perform 9.16 “How do I create an NFM-P user group?” (p. 249).

END OF STEPS

8.4 How do I import users and groups from NFM-P?

8.4.1 Purpose

NFM-P users must be imported to the NSP local user database. The Import function migrates all user accounts and user groups from your NFM-P user database into NSP. The imported users become local NSP users. The imported user groups can be assigned roles that provide the users in the groups access to NSP functions and resources.

Note: NSP supports up to 5000 local users.

Imported NFM-P users require new passwords. Users that have an e-mail address receive a random password by e-mail. Users without an e-mail address are assigned a global default password set by the administrator. Each imported user must change the password during the first login attempt after the import. It is recommended that the NFM-P system administrator assign e-mail addresses to users before the import in order to ensure the greatest security.

Before importing NFM-P users, consider the following requirements and limitations:

- If you intend to use e-mail notification of new user passwords, you must ensure that the NSP e-mail server is configured in the NSP system settings. If the e-mail server is not reachable to NSP and some NFM-P users have e-mail addresses configured, the NFM-P user import will not complete successfully.

  The user import process depends on how the user list with e-mail addresses is created in the NSP system. If the e-mail sending fails for the first user with an e-mail address, the remaining users with email addresses are not imported.
- If NFM-P is configured with remote authentication sources, those authentication sources must be configured in the NSP GUI.
- The NFM-P user parameters imported to NSP are: user name, description, user group, account state, and e-mail address.
- All NFM-P user IDs are converted to lowercase upon import. If two NFM-P user IDs are identical except for case, only one of them is imported. You must clean up any duplicate user IDs in NFM-P prior to import to ensure that all users are imported.
- NSP user groups are case sensitive, as are NFM-P user groups. When NFM-P user groups are imported to NSP, they keep uppercase and lowercase characters. For example, if NFM-P has user groups GROUP1, Group1 and group1, all three are imported into NSP.
- Any NFM-P user names that conflict with existing NSP local users are not imported and do not cause any change to local users.
- To ensure that only necessary users are included in the migration, clean up your NFM-P user database before importing to NSP.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- NFM-P remote users are not imported into NSP (remote users include NSP, LDAP, RADIUS, and TACACS users that have access to the NFM-P GUI.)
- NSP authentication does not support local and remote user authentication for the same user ID. To preserve the use of a remote user ID, the local user ID must be changed to a unique value.

8.4.2 Steps

1

Open **Users and System Security**.

2

Select **Users** from the drop-down list on the toolbar.

3

Click ⋮ **More actions**, **Import NFM-P users and groups**.

4

In the Temporary password for imported Users form, specify and confirm a global temporary password for all imported users.

The global temporary password is only applied to imported users with no e-mail address.

5

Click OK.

The imported users are listed in the Users view. The imported user groups are listed in the User groups view.

6

The NFM-P imported users can now log in to NSP. All imported users will be required to change their password during first login. NFM-P users that have an e-mail address must check their e-mail for their random login password.

Note: In the event that the import fails for certain users or user groups, you can investigate problems in the nspos-tomcat pod logfile at: **`/opt/nsp/os/tomcat/logs/AccessControlApi.log`**

END OF STEPS

8.4.3 Post-import considerations

After importing users from NFM-P, be aware of the following requirements and limitations:

- An imported NFM-P user group that had Administrator scope of command in NFM-P must be assigned to a role with administrative privileges in NSP.
- NFM-P XML SOAP OSS users must remain in NFM-P after import to perform XML SOAP OSS transactions with NFM-P. New NFM-P XML SOAP OSS users must be created in NFM-P.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Non-NFM-P XML SOAP OSS users that are imported to NSP can be deleted from NFM-P after import to NSP.
- NFM-P user groups must exist in NFM-P to define user access permissions through span and scope of control profiles.

8.5 How do I set global user session limits?

8.5.1 Purpose

You can configure limits for NSP user sessions such as maximum inactivity time, maximum GUI sessions per user, and so on. These configurations are set globally and apply to all users. They cannot be configured per user.

8.5.2 Steps

1

Open **Users and system security**.

2

Click ⋮ **More actions**, **Settings**.

3

In the Users and System Security Settings form, click **Session settings**.

4

Configure user session limits in any of the following ways:

UI session inactivity timeout [1]	The number of minutes of user session inactivity before the user is automatically logged out of NSP. GUI activity in an NSP session includes any mouse movement, mouse clicks, or typing in an NSP GUI window.
Maximum session time	The absolute maximum length of a user session (in minutes) before the user is automatically logged out of NSP.
Maximum time to complete login	The maximum time allowed (in minutes) for a user to complete an NSP login.
Maximum time to complete login steps	The maximum time allowed (in minutes) for an NSP login sequence that involves multiple steps; for example, if the user must change their password during login.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Maximum UI sessions per user [2]	The maximum number of simultaneous GUI sessions per user account. When this parameter is set to zero, there are no per-user UI session limits. By default, no per-user limits are enabled.
Maximum OSS sessions per user	The maximum number of simultaneous OSS sessions per user account. When this parameter is set to zero, there are no per-user UI session limits. By default, no per-user limits are enabled.
OSS access token lifespan	The number of minutes before an OSS access token expires.

Notes:

1. Some NSP UI views are in continuous communication while in use, and a user session does not become idle as long as the user has that view open, such as when viewing an alarm list.
2. If a user login attempt exceeds the **Maximum UI sessions per user** limit, the sign-in page displays an error message. If you increase the parameter value to allow more sessions per user, refreshing the sign-in page with the error message opens a session using the previously entered credentials.

5

Click **Save**.

END OF STEPS

8.6 What are user password policies?

8.6.1 Introduction

When an operator attempts to sign in to the NSP and a password change is required, the new password must conform to the password policy of the authenticating agent, as described in the following table.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Authenticating agent	Requirement
NSP	User password complexity rules are configurable; the following are the default rules. An NSP local user password must: • have at least ten characters • not be the same as the previous three passwords • include at least one of the following special characters `( ) ? ~ ! @ # $ % & * _ + ^` The colon `:` character must never be used in an NSP password. HTTP clients that will send the password in a POST request must URL-encode certain characters. To include the **%** or **+** character in a password, they must be specified as the escape codes `%25` or `%2B`, respectively. The **%** character is used for URL-encoding special characters and it is handled differently when the NSP system acquires an access token. When a user logs in to the NSP GUI with the % or + character, it is already URL-encoded. The other special characters mentioned here do not require the URL-encoded character representation. Example: If the desired login password is Main%street8, it must be specified as Main%25street8 in an HTTP client POST request. • include at least one lowercase character • include at least one uppercase character • include at least one digit • not be the username • not equal the e-mail address
WS-NOC	When a WS-NOC-authenticated user is prompted to change their password during an NSP login attempt, the password must conform to the WS-NOC password requirements, which are described in the User ID and passwords rules section of the *WS-NOC Platform Feature Guide*.
LDAP, RADIUS and TACACS+	A password-change policy is not applied during an NSP user login attempt. If a password change is required, the user must contact the system administrator for information about the LDAP, RADIUS, or TACACS+ password requirements.

8.7 How do I set local user password requirements?

8.7.1 Purpose

The password policy defines global password requirements for local NSP user accounts, including password contents and length, and expiry and reuse limits. The password policy settings apply only to local NSP user accounts. The password policy does not apply to users managed through external databases, or to IDP users.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.7.2 Steps

1

Open **Users and system security**.

2

Click ⋮ **More actions**, **Settings**.

3

In the Users and System Security Settings form, click **Password policy**.

4

Configure user password requirements in any of the following ways:

Not recently used	Specifies the number of unique password that must be used before the current password can be used again.
Password expiry	Specifies the number of days a password can be used before it expires.
Special characters	Specifies the minimum number of special characters that must be used in the password. Allowable special characters are: **( ) ? @ # $ % & ! * _ + ~ ^** The colon **:** character must never be used in an NSP password.
Lowercase characters	Specifies the minimum number of lowercase characters that must be used in the password.
Uppercase characters	Specifies the minimum number of uppercase characters that must be used in the password.
Digits	Specifies the minimum number of numerical characters that must be used in the password.
Minimum length	Specifies the minimum number of characters that must be used in the password.
Must not be username	Enable this option to prevent the account username from being used as a password.
Must not be email address	Enable this option to prevent the account e-mail address from being used as a password.

5

Click **Save**.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.8 How do I set login protection restrictions?

8.8.1 Purpose

NSP can temporarily or permanently lock out users for login failures. This includes managing repeated failed login attempts, such as in brute force attacks.

Temporary lockout

A user that reaches a specified number of consecutive failed login attempts can be temporarily disabled for a specified wait interval. During the wait interval, further login attempts by the user are not processed. After the wait interval, OAUTH2 processes new login attempts by the user. If user login attempts continue to fail, the login attempts are subsequently disabled for incrementally longer periods, up to a configurable maximum. Temporary lockout protection is configured by default.

Temporary lockout applies to local and external authentication source users.

Permanent lockout

OAUTH2 can automatically lock out a user after a specified number of consecutive login failures. The user is prevented from logging in until an administrator un-suspends the user account.

Permanent lockout applies only to local NSP users, and not to users defined in external authentication sources.

Quick Login protection

The Temporary Lockout and Permanent Lockout functions both include Quick Login protection. This feature prevents unrealistically-fast login attempts that might originate from a tool or script. If a two consecutive login attempts occur in less than a minimum time interval, a brief lockout is enforced before another login attempt can occur.

8.8.2 Steps

1

Open **Users and System Security**.

2

Click ⋮ **More actions**, **Settings**.

3

In the Users and System Security Settings form, click **Brute force detection**.

4

Select a brute force detection mechanism from the **Brute force detection** menu. Based on your selection complete Step 5 or Step 6.

To disable login protection, select **Disabled** from the menu and click **Save**.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Configure Temporary Lockout protection restrictions as follows:

Maximum login failures	Number of allowed login failures before a temporary lockout.
Wait increment (seconds)	Temporary lockout time after maximum login failures failed login attempts is reached.
Maximum wait (minutes)	Maximum temporary lockout duration.
Failure reset time (hours)	Number of hours after which the login failure count automatically resets.
Quick login check (milliseconds)	Minimum interval between two consecutive login failures, below which will enforce a wait period, as specified by the minimum quick login wait parameter.
Minimum quick login wait (seconds)	Lockout duration triggered by a quick login check violation.

6

Configure Permanent Lockout protection restrictions as follows:

Maximum login failures	Number of allowed login failures before a permanent lockout
Quick login check (milliseconds)	Minimum interval between two consecutive login failures, below which will enforce a wait period, as specified by the minimum quick login wait parameter.
Minimum quick login wait (seconds)	Lockout duration triggered by a quick login check violation.

7

Click **Save**.

END OF STEPS

8.9 How do I suspend a user account?

8.9.1 Purpose

You can temporarily suspend a local or remote NSP user account. After suspension, the user will lose access to the NSP system after they logout and login again.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.9.2 Steps

1. Open **Users and system security**.
2. Select **Users** from the drop-down list on the toolbar.
3. In the Users list, select the user account you want to suspend.
4. On the user account item, click ⋮ **Table row actions**, **Edit user**.
5. On the Update User form, set the **Account state** parameter to **Suspended**.
6. Click **Update**.

END OF STEPS

8.10 How do I configure user account event notifications?

8.10.1 Purpose

You can configure policies to send e-mail notifications to users for the following events:

- user account verification
- user account forgotten password reset URL
- user account lockout
- user account imports from NFM-P

For each event type, you can enable or disable e-mail event notifications, and specify the message subject and body.

8.10.2 Steps

1. Open **Users and system security**.
2. Click ⋮ **More actions**, **Settings**.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

In the Users and System Security Settings form, click **Account verification and recovery**.

4

Configure e-mail notifications under any of the following functional areas:

1. Under **Verify email**, enable notifications to send messages to new users to verify their e-mail address. You can type a custom subject line and message body or use the defaults.
2. Under **Forgot password**, enable notifications to send a message with a password change URL to users. You can type a custom subject line and message body or use the defaults.
3. Under **Account lock**, enable notifications to send messages to locked-out users, telling them how to regain access to NSP. You can type a custom subject line and message body or use the defaults.
4. Under **Import NFMP users**, you can type a custom subject line and message body or use the defaults.

   The default message body informs NFM-P users that they now have a user account with NSP, and provides a temporary password for their account.

   The user must have an e-mail address configured on their NFM-P account to receive this message.

5

Click **Save**.

END OF STEPS

8.11 How do I configure a remote authentication server?

8.11.1 Purpose

You can configure LDAP (including Active Directory), RADIUS, and TACACS server instances in NSP to connect with remote authentication servers. 8.12 “Remote authentication server parameters” (p. 173) describes the parameters you encounter for each authentication protocol.

8.11.2 Steps

1

Open **Users and system security**.

2

Click ⋮ **More actions**, **Settings**.

3

In the Users and System Security Settings form, click **Authentication sources**.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

In the Authentication sources form, click **+ Server**.

5

In the Select protocol form, type a name for the server in the **Displayed name** field.

6

Specify the authentication protocol for the server in the **Select protocol** menu.

Additional authentication parameters appear in the GUI, based on the protocol you selected; see 8.12 “Remote authentication server parameters” (p. 173).

7

Do one of the following:

- For an LDAP server, complete Step 8.
- For a RADIUS server, complete Step 9.
- For a TACACS server, complete Step 10.

8

Configure the LDAP server parameters:

a. Configure the connection, user search, and group search parameters using the values specific to the remote LDAP server.

b. Update the NSP TLS certificate for LDAP remote authentication; see 8.25 “How do I update the NSP TLS certificate for remote authentication?” (p. 194).

c. Click **Test connection** to verify the LDAP server protocol, IP address/hostname, and port reachability. This ensures that the server is online and accessible from your network.

If the LDAP server instance is configured with multiple redundant LDAP server URLs, the **Test connection** function tests each server URL in turn and responds with a Reachable message when a server responds.

d. Turn on the **Enable LDAP authentication** option if you want NSP to connect to the LDAP server immediately.

9

Configure the RADIUS server parameters:

a. Configure the connection parameters using the values specific to the remote RADIUS server.

b. Click **Test Connection** to read the IP address/hostname from the Address field and verify the RADIUS server reachability. This ensures that the server is online and accessible from your network.

c. Turn on the **Enable RADIUS server** parameter if you want NSP to connect to the RADIUS server immediately.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10

Configure the TACACS server parameters:

a. Configure the connection parameters using the values specific to the remote TACACS server.

b. Click **Test Connection** to read the IP address/hostname from the Address field and verify the TACACS server reachability. This ensures that the server is online and accessible from your network.

c. Turn on the **Enable TACACS server** parameter if you want NSP to connect to the TACACS server immediately.

11

Click **Submit** to save the server configuration.

END OF STEPS

8.12 Remote authentication server parameters

8.12.1 Purpose

This topic provides descriptions for parameters on LDAP, RADIUS and TACACS server configurations.

8.12.2 LDAP parameters

Connection URL	Connection URL to LDAP server. If you are configuring multiple redundant LDAP servers under this instance, their URLs should all be specified in this field, separated by spaces: ***server_1_URL server_2_URL server_3_URL*** The same server URL may be specified on multiple LDAP server instances.
Type	Authenticated or AD.
Priority	Where multiple LDAP server instances are configured in NSP, the priority value for each instance determines the order in which LDAP servers are used for user authentication. Lowest number is highest priority.
Timeout	Timeout interval for receiving response from server, in milliseconds.
Bind DN	DN for the LDAP admin.
Bind credential	Password for LDAP admin.
Username LDAP attribute	Name of the LDAP attribute for user name.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

RDN LDAP attribute	Name of LDAP attribute used as RDN of typical user DN.
UUID LDAP attribute	Name of LDAP attribute used as unique object identifier.
User object classes	All values of object classes for users.
Search scope	User search is one level or subtree in LDAP server.
User DN	Full DN of LDAP tree where your users are located.
User filter	Additional LDAP filter for filtering searched users.
Groups LDAP filter	Additional filter for group search.
Group name LDAP attribute	Name of LDAP attribute used on group objects.
Group DN	DN where groups are located in LDAP tree.
Preserve group inheritance	Set to Disabled for flat user group structure.
Group membership attribute type	Set to DN or UID DN specifies that group members are declared in their full distinguished name format. UID specifies that group members are declared in user ID format. If you set UID format, the Preserve group inheritance option is disabled.
Group object classes	Object classes for group records.
Group membership LDAP attribute	Name of LDAP attribute on group used for membership mappings.
Group membership user LDAP attribute	Name of LDAP attribute on the user used for membership mappings.
Group member of LDAP attribute	Name of LDAP attribute on LDAP user which contains the groups.

8.12.3 RADIUS parameters

Address	IP address or hostname with port
RADIUS shared secret	Shared secret to connect with RADIUS server
Timeout	Timeout interval for receiving response from server, in milliseconds
Retry count	Maximum number of attempts for connecting to RADIUS server
Protocol	PAP or CHAP
Vendor ID	Vendor ID in RADIUS, integer
Role VSA ID	Role ID in RADIUS, integer
NAS ID	Network access server ID (optional)
NAS IP	Network access server IPv4 address (optional)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NAS IP V6	network access server IPv6 address (optional)

8.12.4 TACACS parameters

Address	IP address or hostname with port
TACACS shared secret	Shared secret to connect with TACACS server
Timeout	Timeout for receiving response from server, in milliseconds
Protocol	PAP or CHAP
Role VSA ID	Role used for VSA search
VSA service ID	VSA search service identifier

8.13 How do I configure a remote identity provider?

8.13.1 Purpose

NSP can use OpenID Connect and SAML identity providers for user authentication to NSP. You can configure an OpenID Connect or SAML server in NSP. After you have enabled and submitted an IDP configuration in NSP, a cross-launch link to the IDP appears on the NSP login page. If you configure multiple IDP instances, there will be a list of cross-launch links at login.

Once IDP configuration is complete, users or IDP administrators can configure direct URL access into NSP; see 8.14 “How do I configure a direct URL to NSP for IDP users?” (p. 178).

The parameters you encounter for each IDP protocol are described at the bottom of this topic.

8.13.2 Steps

1

Open **Users and system security**.

2

Click ⋮**More actions**, **Settings**.

3

In the Users and System security settings form, click **Identity provider**.

4

The Identity provider form displays a list of any configured IDP servers. If you click ⋮**More**, **Show Metadata** on a SAML IDP server item in the list, the complete SAML service provider metadata is displayed in XML format in a popup window. You can copy the metadata to the clipboard and paste it into a new SAML IDP server configuration.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Click **+ Server**.

6

In the Select protocol form, type a name for the IDP in the **Displayed name** field.

This name appears as a redirect link on the NSP login page.

7

Specify the authentication protocol for the IDP in the **Select protocol** menu.

Additional authentication parameters appear in the GUI, based on the protocol you selected.

8

Do one of the following:

- For a SAML IDP, complete Step 9.
- For an OpenID Connect IDP, complete Step 10.

9

Configure the SAML IDP parameters:

a. Configure the connection parameters using the values specific to the remote SAML IDP.

b. Click **Test Connection** to read the IP address/hostname from the configuration and verify the SAML IDP reachability. This ensures that the IDP is online and accessible from your network.

c. Turn on the **Enable SAML authentication** option if you want NSP to connect to the SAML IDP immediately.

10

Configure the OpenID Connect IDP parameters:

a. Configure the connection parameters using the values specific to the remote OpenID Connect IDP.

If you configure multiple OpenID Connect IDPs, each one must have a unique IP address or hostname.

b. Update the NSP TLS certificate for OpenID Connect remote authentication; see 8.25 “How do I update the NSP TLS certificate for remote authentication?” (p. 194).

c. Click **Test Connection** to read the IP address/hostname from the configuration and verify the OpenID Connect IDP reachability. This ensures that the IDP is online and accessible from your network.

d. Turn on the **Enable openID connect authentication** parameter if you want NSP to connect to the OpenID Connect identity provider immediately.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Click **Submit** to save the identity provider configuration.

END OF STEPS

8.13.3 SAML parameters

GUI order	In an NSP deployment with multiple IDPs, this integer specifies the position of the SAML IDP redirect link in the link list on the NSP login page.
Alias	The alias is a unique identifier for the SAML IDP, and is used to build the redirect URI.
Entity ID	The entity ID is a unique identifier for the SAML service provider.
IDP entity ID	The IDP entity ID used to validate the issuer for received SAML assertions. If empty, no issuer validation is performed.
Single sign on service URL	The URL used to send authentication requests (SAML AuthnRequest).
Enable HTTP-POST binding for AuthnRequest	Option to use an HTTP-POST for Authentication Request with the SAML server (data is in the body of HTTP POST request).
Enable HTTP-POST binding response	Option to use an HTTP-POST in the SAML response (data is in the body of the HTTP POST response).
Allowed clock skew (seconds)	Allowed time difference between IDP and NSP system that is tolerated when validating identity provider tokens. Default value is zero.

8.13.4 OpenID Connect parameters

GUI order	In an NSP deployment with multiple IDPs, this integer specifies the position of the OpenID Connect IDP redirect link in the link list on the NSP login page.
Alias	The alias is a unique identifier for the OpenID Connect IDP, and is used to build the redirect URI.
Client ID	The client identifier registered with the IDP.
Client secret	The client secret registered with the IDP.
Authorization URL	URL used to redirect users for authentication. This URL is used to initiate the OIDC authentication process.
JWKS URL	URL endpoint that is used to retrieve public keys required to verify identity tokens for OIDC authentication.
Token URL	URL/end point that is part of the OIDC flow. Provides the necessary tokens after successful authentication.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

User info URL	URL used to retrieve authenticated user profile information after successful authentication via OIDC.

8.14 How do I configure a direct URL to NSP for IDP users?

8.14.1 Purpose

Users that login to an identity provider application can access NSP directly via a URL bookmarked in their browser, bypassing the NSP login page. An IDP administrator can include the URL in an IDP landing page to open NSP directly.

8.14.2 Steps

1

The URL for direct NSP launch is configured as follows:

https://*NSP_IP*/auth/realms/Nokia/protocol/openid-connect/auth?client_id=*NSP*&kc_idp_hint=*alias*&response_type=none&redirect_uri=https%3A%2F%2F*NSP_IP*/web

where

NSP_IP is the NSP IP address or hostname

alias is the SAML or OIDC alias for the IDP

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP User Access Control

8.15 What is User Access Control?

8.15.1 Overview

User Access Control (UAC) defines the commands a user can perform in an NSP system and the objects on which those commands can be performed. NSP UAC is defined through role definitions that are assigned to user groups, and each user is associated with one user group.

In an NSP deployment, UAC applies to a user when accessing NSP functions. Access is assigned at the NSP level and applies across the NSP GUI. Users see their specified NSP access permissions enforced when they login to NSP. The user access configuration specified in NSP is enforced **in place of** any pre-existing access control setup (from NFM-P or WS-NOC). Local NSP user access to NSP resources is always controlled through NSP, regardless of whether UAC is enabled or not. As a network evolves, an NSP administrator must create or modify user groups, roles, and resource groups to provide the required user access to NSP functions. Be aware of functional cross-dependencies.

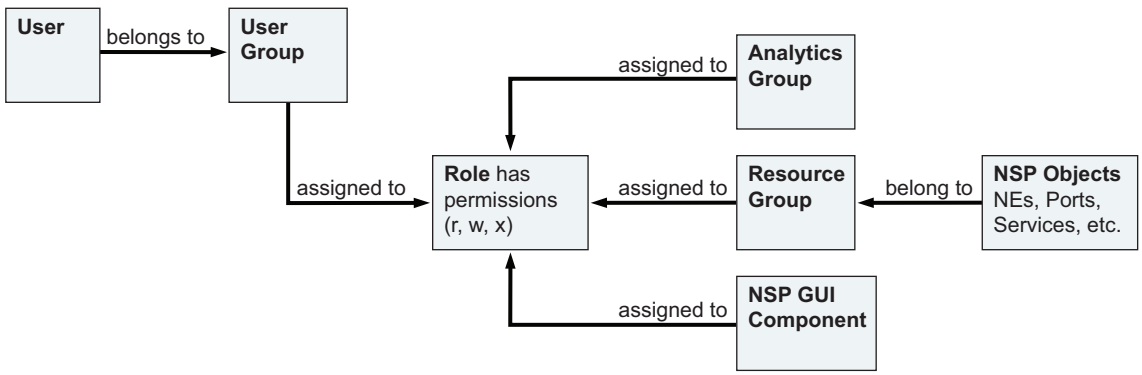
NSP UAC is disabled by default, meaning that users can access any NSP function that is not restricted by a specific user group requirement. Users that belong to the admin user group can access all functions, including admin-only functions. Users that do not belong to the admin user group can access all non-admin applications. A user that does not belong to the admin user group but has a system administrator role privilege will not be able to access admin-only functions. When UAC is enabled, it controls user access to NSP functions independently of the user management systems in NFM-P or WS-NOC.

When NSP UAC is enabled, the role definitions belonging to an NSP user group determine the NSP functions and commands a user can access, and which network objects the user can access.

In CLM deployments, UAC applies to CLM users.

NSP users that access NFM-P or WSNOC have access determined by what is configured for that user group in NFM-P or WSNOC applications. (eg. An NSP user accessing NFM-P will have access to the NFM-P scope and span profiles that belong to the user's NFM-P user group).

Figure 8-1 User Access Control architecture



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.15.2 Roles

A role object specifies which resources and NSP functions its associated user groups can access. Network resource access is assigned to a role through resource groups, while functional access and Analytics resource access are specified directly on a role object.

NSP administrator role

A predefined NSP administrator role, user group, and admin user account are automatically created during NSP system installation and cannot be modified. The admin user has full access to all NSP functions and resources, and can define the roles and resource groups that are assigned to user groups. The admin user can create additional roles with the Administrator designation, which carries the same unlimited functional and resource access.

8.15.3 User groups

A user group associates a group of NSP users with one or more roles, thereby enabling user access to functional areas and resources. Administrators create user groups and assign roles to them, according to the type of network activities the user group is meant to perform. When a role is assigned to a user group, all users within the group have the same access to resources and functions, as specified on the role. A user group can be assigned multiple roles to allow broader access rights for its users.

Individual NSP users can be created by external authentication sources or IDPs, where users are assigned to corresponding user groups. In order for the members of a user group to have access to NSP resources and functions, the user group name returned by the authentication source or IDP must exactly match a corresponding user group name in NSP.

Local NSP users and user groups can also be created in the NSP.

Users requiring WS-NOC access require a user group assignment that maps to a predefined WS-NOC role; for information, see *To map external user groups to predefined WS-NOC roles* in the *NSP Installation and Upgrade Guide*.

8.15.4 Resource groups

A resource group is a collection of network equipment or services which can be assigned to a role. The role is assigned to a user group, thereby granting the user group access to the network resources in the resource group. Network resource groups are defined in Resource Groups.

8.15.5 UAC for Log Viewer

All NSP users have basic read-only access to Log Viewer. You can configure Log Viewer with custom roles that allow additional user privileges. You configure a custom role in Log Viewer and then associate it with an NSP user group, thereby granting enhanced access within Log Viewer to the group members; see 8.22 “How do I configure user access in Log Viewer?” (p. 189)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.16 Pathway: Configure User Access Control

8.16.1 Purpose

This pathway describes the recommended order of tasks to configure UAC across NSP. The sequence of tasks outlined here is especially recommended if you are setting up UAC in NSP for the first time. Once you have UAC deployed in NSP, you can configure your user groups, roles, and resource groups in any order.

8.16.2 Steps

Prerequisite: create group directories and resource groups

1

You create group directories and resource groups in Resource Groups. Resource groups (of NEs, ports, LAGs, or services) are applied to role objects to grant user access rights to network resources. See 8.38 “How do I create a group directory?” (p. 205) and 8.39 “How do I configure a resource group?” (p. 206)

Optional: configure Analytics reporting

2

If you intend to use NSP Analytics reporting, you must fully configure Analytics before you to configure Analytics resource access in your roles. You cannot configure resource access on a role if Analytics is not enabled in the NSP configuration.

Create roles

3

Create roles according to the type of tasks your user groups will be performing, and the types of resources they will need to access. A role object specifies access rights to specific NSP functions and resources; see 8.18 “How do I configure a role?” (p. 184)

Import or create users and user groups

4

Choose one of the following options:

- Create local NSP users; see 8.3 “How do I configure an NSP user?” (p. 159).
- If you have a user access control configuration from NFM-P, it is strongly recommended that you import your users and user groups from NFM-P. This ensures that all of your existing users are included in the new access control setup, and helps ensure a seamless transition from the NFM-P; see 8.4 “How do I import users and groups from NFM-P?” (p. 162).
- If you are configuring user access control for a remote authentication source, create new user groups; see 8.20 “How do I configure a user group?” (p. 188).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Enable UAC

5

Note: When you enable UAC in NSP, individual users will see their specified access rights enforced when they login to NSP. The user access configuration you create are enforced **in place of** any previous access-control setup, except in the NFM-P and WS-NOC, which each employ local user management. Local NSP user access to NSP resources is always controlled through NSP, regardless of whether UAC is enabled or not.

Once you have configured and reviewed your user groups and their associated roles, you can enable UAC; see 8.23 “How do I enable User Access Control?” (p. 190)

END OF STEPS

8.17 How do I configure alarm access using roles?

8.17.1 Purpose

Users can manage alarms for objects that are included in the resource groups assigned to their roles. The tasks that users can perform depend on the access level provided to the resource groups. Consider the following:

- Network objects that have multiple endpoints or components, such as SAPs, require access to all endpoints for alarm management. For example, users can only see alarms on physical links when they have access to both endpoints.
- Viewing alarms on service-related objects requires access to the parent service and associated equipment.
- In some cases, access level can be inherited from the parent object. For example, when no access level is granted for a port, any level of access granted to the parent NE will grant the same access level to the port.
- In the Unhealthy NEs view, users must have access above “none” to view any NEs that might appear in the page.

The following table describes in more detail how the access levels of resource groups determine the type of alarm management tasks that users can perform.

Resource groups[1]	Access level “none”	Access level “read”	Access level “write”	Access level “execute”
Equipment→Port	Port access is equal to the parent NE access.	• Can see alarms on ports and associated SAPs if the user has access to the corresponding service. • Can see alarms on physical links if the user has access to both endpoints.	Can open affected object and impacted object.	Can open affected object and impacted object.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Resource groups[1]	Access level “none”	Access level “read”	Access level “write”	Access level “execute”
NE	No access to alarms on the NE and equipment.	• Can see alarms on the NE and its equipment. Can see alarms on service sites and SAPs when the user has access to the corresponding service. • Can see alarms on physical links if the user has access on to both endpoints. • Can see alarms on LSPs if users have access to both endpoints.	Can open affected object and impacted object.	• Can open NE sessions for the affected NE. • Can open affected object and impacted object.
Service	No access to alarms on service and associated service object.	• Can see alarms on service. • Can see alarms on associated service objects only if the user has access to the corresponding equipment, including NEs and ports (SAPs, sites, tunnel bindings).	Can open affected object and impacted object.	• Can open affected object and impacted object.

Notes:

1. Resource group alarm access for LAG groups is not currently supported.

The following pathway describes the high-level steps required to create a role intended for alarm management, and to assign it to a user group. This pathway applies to all NSP users who need to view object alarms, regardless of which NSP UI they use for alarm viewing.

8.17.2 Steps

Create resource groups

1

Create an NE | port | LAG group directory; see 8.38 “How do I create a group directory?” (p. 205)

2

Create an NE | port | LAG resource group in the group directory, and define a filter that includes the network elements the user needs to view; see 8.39 “How do I configure a resource group?” (p. 206)

3

Create a service group directory; see 8.38 “How do I create a group directory?” (p. 205)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Create a Service resource group in the service group directory, and define a filter that includes the services the user needs to view. You can create multiple service resource groups within a group directory; see 8.39 “How do I configure a resource group?” (p. 206)

You can create the service resource group based on a Site ID (NE system address) to include all services for the associated NE.

Assign resource groups to roles

5

Add the resource groups to a role; see 8.18 “How do I configure a role?” (p. 183).

6

Assign the role to the appropriate user group; see 8.20 “How do I configure a user group?” (p. 188).

END OF STEPS

8.18 How do I configure a role?

8.18.1 Purpose

A role object specifies access rights to specific NSP functions and network resources. Roles are assigned to user groups, bringing all access rights defined on the role to all members of the user group.

Consider the following before configuring a role:

- If you intend to assign resource group access to a role, you must configure your resource groups before completing this procedure.
- If you intend to assign Data Collection and Analysis resource access in this role, you must first configure Data Collection and Analysis, and must assign Read/Write/Execute permission to the Analyze/Assure or Data Collection and Analysis category.
- A user with access to device discovery must also be given access to device management. Device management access is required to view discovered devices.

Note: Do not confuse the Access settings with the Deployment Control settings that are configured in the NSP settings; the Deployment Control settings determine which NSP views are activated and available.

8.18.2 Steps

1

Open Users and System Security.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Select **Roles** from the drop-down list on the toolbar.

3

Click **+Create role**. The Create Role form opens.

4

In the Identification panel, specify a role name and description.

The **Role Name** and **Description** fields can employ **only** the following special characters: **- _ . @**

The Role Name string must not contain *any* spaces, including a leading or trailing space.

5

In the Characteristics panel, you can enable the Administrator designation for the role.

To create an administrative role with access to all resource groups and function, enable the **Administrator** check box.

If you enable this option, no further steps are necessary. Click **Create** to save the role.

6

To assign NSP functional access to the role, go to the Action permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role. For a description of the access permissions, see 8.24.2 “NSP action permissions” (p. 192).

If you intend to assign Data Collection and Analysis resource access in this role, you must assign Read/Write/Execute permission to Data Collection and Analysis.

7

To assign network resource access to the role, go to the Resource groups access panel. (For a detailed explanation of the Resource groups access panel, see 8.19 “How do I set network resource access levels?” (p. 186).)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these.

a. You can assign resource group access globally by resource type. Enable either or both options:

- **Access to all equipment** assigns full permissions on all NE resource groups and port resource groups to the role.
- **Access to all services** assigns full permissions on all service resource groups to the role.

b. Expand the resource group category for resource groups you want to include in the role. (For a detailed explanation of the Network resource access panel, see 8.19 “How do I set network resource access levels?” (p. 186).)

- Select an access level from the drop-down list for each resource type you want to include in the role.
- If you specify an access level to a resource group category, all resource groups within the

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

category are included in the role at the same access level.
If the Group category list is empty or the resource group you are looking for does not appear, you can create resource groups in Resource Groups.

8

To assign Analytics resource access to the role, go to the Analytics resource access panel.

In order for the Analytics Resource Access panel to appear, Analytics reporting must be enabled and configured in NSP and you must assign Read/Write/Execute access to Analytics in this role.

Assign access to Analytics categories or individual Analytics resources in the Analytics repository list:

- To obfuscate specific Analytics report data for user groups associated with the role, enable the **Data anonymization** check box.
- Assign access to an entire Analytics category from by enabling the associated **Permissions** check box ☑.
- Assign access to individual Analytics resource items by expanding an Analytics category, selecting an Analytics resource, and enabling its corresponding **Permissions** check box ☑.
  Some Analytics categories have nested subcategories, each containing individual Analytics resources. An Analytics category or subcategory with access granted on all contained resources is displayed as fully-enabled ☑. If access is granted on only some contained resources, it is displayed as partially-enabled ▣.

Note: The View/Execute permissions for a report in an Analytics report repository do not apply to drill-downs.
For example, a user group has View/Execute permission for report A but no permission for report B. If report B is a drill-down from report A, users will be able to execute report A via report B, although this might not seem obvious.

9

Click **Create** to save your changes and return to the Roles list.

END OF STEPS

8.19 How do I set network resource access levels?

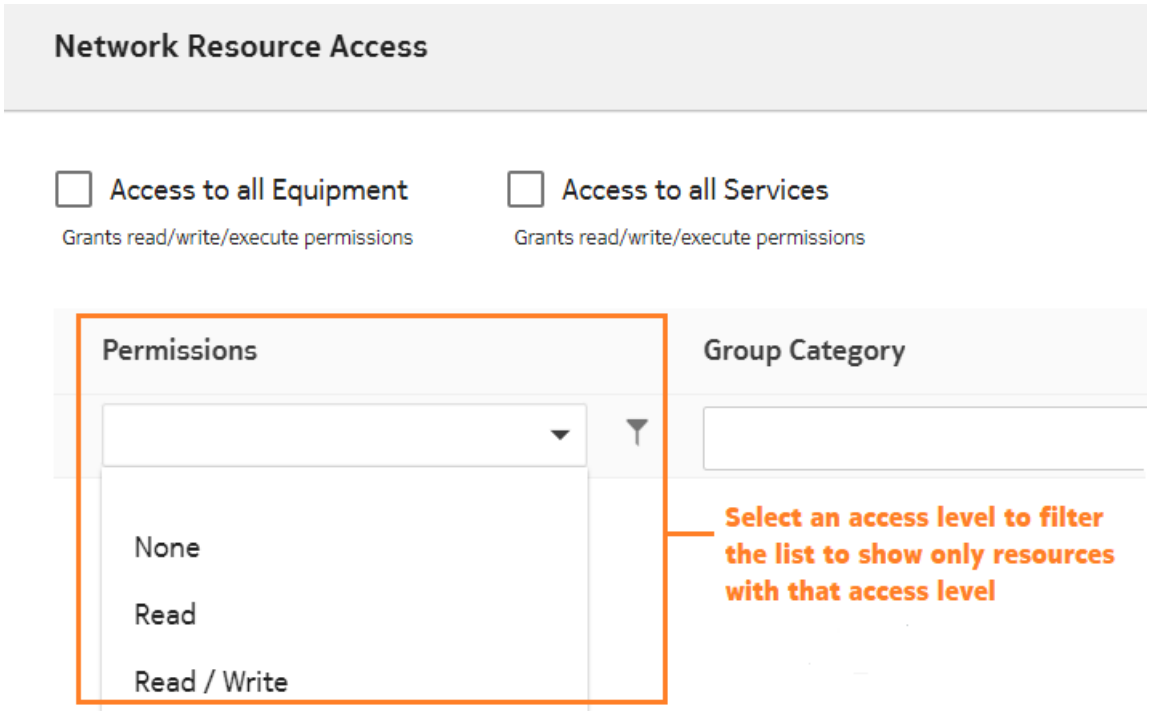
8.19.1 Overview

This topic describes the features of the Resource Groups Access panel in the Create Role form. You can search for specific resources and you can search for resources with a common access level. Use this topic as a reference when performing the 8.18 “How do I configure a role?” (p. 184) procedure.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.19.2 Filter the list

You can filter the network resource list to a specific access level by selecting an access level from the drop-down list at the top of the Permissions column. The list is reduced to show only resources that have the same access level. The filter is set to a null value (no access level selected) by default so that all available resources are displayed in the list.



8.19.3 Search the list

You can search the resource list by typing a string in the Search field at the top of the Group Category column. The list updates dynamically with matching entries as you type.

8.19.4 Set access permissions on a category

You can set global access permissions on an entire category of resources. Select an access level from the drop-down list next to a resource group category. The access permissions are set to the same level for all resources in the category.

8.19.5 Set access permissions on an individual item

You can set access permissions on a single resource group. Expand the resource group and then select an access level from the drop-down list next to a resource group.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.20 How do I configure a user group?

8.20.1 Purpose

A user group is a definition of user roles and associated access rights. You assign NSP GUI and resource access rights to a user group through role objects. When a role is assigned to a user group, all access rights defined on the role are assigned to the user group.

To configure a complete user group, you must configure the roles before performing this procedure; see 8.18 “How do I configure a role?” (p. 184)

8.20.2 Steps

1

Open Users and System Security.

2

Select **User groups** from the drop-down list on the toolbar.

3

Click ＋**Create user group**. The Create user group form opens.

To make changes to an existing user group, select the group in the list and click ⋮**Table row actions**, **Edit user group**. The Edit user group form opens.

4

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The **User group name** and **Description** fields can employ **only** the following special characters: **- _ . @**

The **User group name** string must not contain *any* spaces, including a leading or trailing space.

5

To assign user roles to the group, click ＋**Add roles** on the Roles panel. The Add roles form opens.

6

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the **Selected roles** list.

To remove a role item from the **Selected roles** list, click **Delete** on the item.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Click **Create** to save your changes and return to the User groups list.

END OF STEPS

8.21 How do I configure a default user group?

8.21.1 Purpose

The default user group is intended as a holding group for remote NSP users who attempt to login to NSP with no user group assigned to their account. Such users are automatically assigned to the default group, and have access to the NSP GUI in accordance to the roles assigned to the default group.

You can designate any existing user group as the default group, or you may choose to create a new user group specifically to use as the default; see 8.20 “How do I configure a user group?” (p. 188).

8.21.2 Steps

1

Open **Users and System Security**.

2

Click ⋮ **More actions**, **Settings**.

3

In the Users and System Security Settings form, click **Global access control**.

4

Select a user group from the **Default user group** drop-down menu.

5

Click **Save** to save default user group configuration.

END OF STEPS

8.22 How do I configure user access in Log Viewer?

8.22.1 Purpose

This procedure describes how to grant NSP users enhanced access to Log Viewer. You must create special (non-NSP) roles within Log Viewer that specify access permissions within Log Viewer. These roles are mapped to an NSP user group, granting enhanced access to the group members, over and above the basic read-only access they already have within Log Viewer.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Detailed documentation on how to specify permissions in Log Viewer roles is available in the Log Viewer documentation, which can be accessed from the Log Viewer GUI.

8.22.2 Steps

1

Open System Health.

2

Open Log Viewer / Security / Roles

3

In the OpenSearch Dashboards, Overview screen, select **Security** from the main menu.

4

In the Get Started screen, select **Roles**.

5

In the Roles screen, click **Create role**.

6

In the Create Role screen, specify a name and set permissions for the role.

7

Click **Create**.

8

In the updated Role form, click **Mapped users**.

9

In the Mapped Users screen, click **Map users**.

10

Enter an NSP user group name in the **Backend roles** field and click **Map**.

END OF STEPS

8.23 How do I enable User Access Control?

8.23.1 Purpose

Note: When you enable user access control, individual users will see their NSP access rights enforced when they login to NSP.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The user groups and roles you create are enforced **in place of** any previous access-control setup, except in the NFM-P and WS-NOC, which each employ local user management.

8.23.2 Steps

1

Open Users and System Security.

2

Click ⋮ **More actions**, **Settings**.

3

In the Users and System Security Settings form, click Global Access Control.

4

Turn on the **Enable user access control** option and click **OK** in the Warning pop-up.

5

Click **Save** to enable access control.

END OF STEPS

8.24 What are NSP operator roles and responsibilities?

8.24.1 NSP operators

Operator responsibilities determine whether you assign Read or Write privileges to the resource groups of an associated role. For example, the administrator role has Write privileges to all resources. A user with an assigned network operator role, however, may have Read access to the NEs in multiple resource groups for troubleshooting purposes, but be granted Write access only to the resource group for the NEs that they maintain.

Note: When only functional access is configured in a role that has no assigned resource groups, the role has full access to all resource groups.

The following table lists and describes typical network operator roles and responsibilities as examples for NSP role creation.

Role	Responsibilities
Administrator	User Access Control, network monitoring, system administration
Network operator	Network fault detection and troubleshooting, equipment health and service infrastructure monitoring
Service operator	Multi-layer service provisioning

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Role	Responsibilities
Network engineer, traffic path	Routing management, optimization, and planning
Network engineer, cross-domain	Network connectivity, optimization, and planning
Network engineer, provisioning	Device configuration, NE software and script management

8.24.2 NSP action permissions

Action Permissions are settings that control what users can see and do within different NSP modules. Permissions are configured per module and will include some or all of: None, Read, Read & Write, Read & Execute, Read Write & Execute. For some modules, additional action permission scopes are available when Read is selected.

The following table lists the NSP action permissions.

Action permission	Description	Reference
NSP Notification Service	Access to Northbound Interface (NBI) notifications.	
Analytics Reports	Access to reports created from raw or aggregated data collected using the NFM-P or NSP telemetry.	
Data Collection and Analysis Management	Access to telemetry subscriptions, aggregation and age-out policies, baselines, and indicators. Also provides access to OAM tests, templates, test suites, test results, and configuration objects when combined with the OAM Tests permission.	
Device Management	Access to managed NEs, ZTP process, configuration deployments, configuration templates, configuration intent types, operations, operation schedules, operation types, and NE images.	See the user access control information in “How does NSP support devices?” in the *NSP Device Management Guide*.
File Server	Access to a utility for importing and managing files required by various NSP functions.	

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Action permission	Description	Reference
Network Intents	Access to intent artifacts, mediators, and policies. This will affect CRUD, lifecycle management, and import capabilities.	See the access control information in “What is an intent type?” in the *NSP Network Automation Guide*. User access can also be configured on a per intent type basis; see “How do I configure user access to an intent type?”
Network Inventory	Access to the NE Inventory view: a tree of configured equipment (shelf, card slot, card, port) and logical objects (link aggregation groups, routing instances, ACL sets, BFD) on a selected NE.	—
Model Driven Configurator	Access to configure parameters and view state information on NEs managed by MDM for which MDC adaptors have been installed.	—
Device Discovery	Access to NE discovery rules, mediation policies, and reachability policies.	See the access control information in “How does device discovery work?” in the *NSP Device Management Guide*.
Network Security	Access to the Anti-theft policies view The Manage anti-theft policies additional scope enables the user to create, edit, and delete anti-theft policies.	
OAM Tests	Access to OAM tests, test templates, test suites, test results, and configuration objects. Access is available in Data Collection and Analysis Management when combined with the Data Collection and Analysis Management role.	
Service Management	Access to tunnel templates, service templates, tunnels, services, customers, and steering parameters.	“How does service management implement user access control?” in the *NSP Service Management Guide*.
System Health	Access to Role Manager and ASM APIs. System Health GUI is administrator access only.	

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Action permission	Description	Reference
Workflows	Access to workflow artifacts, actions, environment variables, executions, and triggers. This will affect CRUD, execution management, trigger management, and debugging capabilities.	See the access control information in “What are Workflows?” in the *NSP Network Automation Guide*. User access can also be configured on a per workflow basis; see “How do I configure user access to a workflow?”
Device Configuration	Access to configuration deployments, configuration templates and configuration intent types. Device Configuration also requires access to the Device Management module.	See the access control information in “What is device configuration in NSP?” in the *NSP Device Management Guide*.

Notes:

1. NSP GUIs and functions that were previously accessible to all users will have an auto-created role enabling user access when upgrading to an NSP release where GUIs/functions become RBAC controlled.

8.25 How do I update the NSP TLS certificate for remote authentication?

8.25.1 Purpose

The TLS certificate for LDAPS or OpenID Connect remote authentication must be current, or the remote authentication attempts fail.

Perform this procedure if the TLS certificate of the LDAPS or OpenID Connect remote authentication server is updated.

CAUTION

Service Disruption

Performing the procedure requires a restart of each NSP cluster, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period.

Note: You must perform the procedure on each NSP cluster.
In a DR deployment, you must perform the steps first on the standby NSP cluster.

8.25.2 Steps

1

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Obtain the new authentication server TLS certificate.

2

Ensure that the authentication server TLS certificate is specified in the trustedCertificates parameter in nsp-config.yml:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

Example:

trustedCertificates: ["/opt/certs/ldap.pem", "/opt/certs/openid.pem", "/opt/certs/*otherCert*.pem"]

Where trustedCertificates is the parameter name and the values in square brackets are the file names of the certs to process into the configuration. The above example includes the paths to the **ldap.pem** and **openid.pem** authentication server TLS certificates.

3

Open a terminal session to the NSP deployer VM and log in as the root or NSP admin user.

4

Enter the following to apply the certificate:

/opt/nsp/NSP-CN-DEP-*release-ID*/bin/nspdeployerctl install --config --deploy ↵

5

Restart the Keycloak pod.

1. Log in as the root user on the NSP cluster host.
2. Enter the following:

   # kubectl get pods -A | grep nspos-keycloak ↵

   The following Keycloak pod information is displayed:

   ```
   namespace   nspos-keycloak-pod_ID  n/n  Running  1 (timespan
   ago)  timespan
   ```
3. Record the *pod_ID* value.
4. Enter the following:

   # kubectl delete pod nspos-keycloak-*pod_ID* -n $(kubectl get pods -A | awk '/nspos-keycloak-*pod_ID*/ {print $1;exit}') ↵

   where *pod_ID* is the Keycloak pod ID recorded in substep 3

   The Keycloak pod restarts, and the updated certificate is put into effect.

6

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

User session management and logging

8.26 What is user session management?

8.26.1 User sessions

The session management function lets administrative users monitor active user sessions in NSP. The Sessions GUI lists all active NSP user sessions and RESTCONF API sessions.

Administrative users can manually terminate one or more user sessions and send messages to one or more active NSP users. Messages would typically be sent to forewarn users of an upcoming session termination, or for other operational events in the NSP system. Messages appear in any NSP views the recipient users have open. Messages are flagged as Information, Warning, or Urgent. Recipient users must have NSP open on their desktop to receive messages.

Note: You cannot send messages to RESTCONF API sessions because they do not involve actual users. Exercise caution in terminating RESTCONF API sessions, as they often involve critical network functions.

8.26.2 User activity logging

Administrators can use the NSP user activity logging function to monitor users' actions across NSP functional areas. NSP user actions are logged in the Users and System Security, User Activity Logs view, including actions invoked through RESTCONF APIs or NSP UIs.

NSP user event logs contain the following types of information:

- identity of user associated with event
- event type (configuration change, file access, etc.)
- executed operations and their results
- event time

You can retain activity logs for up to 365 days, with up to 10 000 000 log events, as configured in the User Activity Logs settings. You can also export activity logs to an external file for archival purposes.

Note: The NFM-P and WS-NOC activity logging functions run separately from NSP activity logging.

8.27 How do I terminate user sessions?

8.27.1 Steps

1

Open Users and System Security.

2

Select **Sessions** from the drop-down list on the toolbar.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

To terminate a single session, select a user session in the list and click **Terminate** on the right-hand side of the item.

4

To terminate multiple sessions, press the Ctrl key and click on the session items you want to terminate, and then click **Terminate session** on the toolbar.

You can clear selections by clicking **Deselect all** on the toolbar.

5

At the prompt, confirm the session termination.

END OF STEPS

8.28 How do I send a message to active users?

8.28.1 Steps

1

Open Users and System Security.

2

Select **Sessions** from the drop-down list on the toolbar.

3

Do one of the following:

1. To send a message to one user, select a user session in the list and click **Table row actions**, **Send message** on the right side of the item.
2. To send a message to all active users, click **Send broadcast message** on the toolbar.

4

In the message form that opens, select a message type and then type your message text in the box.

5

Click **Send**.

A confirmation message appears.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: Although a message may be confirmed as Sent, this does not guarantee that the message is received by all users. Under some circumstances (user logged out, browser window closed, etc.) some users may not receive the message.

END OF STEPS

8.29 How do I view user events?

8.29.1 Purpose

This procedure describes basic user event viewing options.

8.29.2 Steps

1

Open Users and System Security.

2

Select **User activity logs** from the drop-down list on the toolbar.

The User activity logs list displays a list of user events over a specified time period (All available, by default).

3

Use any of the following viewing options to control what you see in the log:

- **Change the log event time period:** Click and specify a new time period.
- **Filter the log under a specific column:** Type a text string in the text field at the top of a column and press Enter.

  When typing a search string for the User Name column, you must type a complete, case-sensitive, user name. For other columns, you can type a partial search string.
- **Sort the log under a specific column:** Click on a column header to sort the list under that column, in alphabetical or numerical order. Click the column header a second time to reverse the sort order. Click the column header a third time to clear sorting under that column.

4

To view details about a specific log event, click on the event item in the log.

The Info panel displays expanded information about the event, including the name of the user who executed the event, affected objects, and affected parameters.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.30 How do I filter the event log view?

8.30.1 Purpose

Create advanced filters to reduce the log view to specific events that you want to investigate. Using Boolean filter expressions, you can create and combine filters to narrow log events to very specific parameters.

8.30.2 Steps

1

Open Users and System Security.

2

Select **User activity logs** from the drop-down list on the toolbar.

The User activity logs list displays a list of user events over a specified time period (All available, by default).

3

On the User activity logs list, click **Add filter** and select **Advanced filter**. The Advanced filter form opens.

4

Type a filter name and description.

5

Type a Boolean filter expression in the **Filter expression** field, starting with a log information attribute type, followed by a Boolean operator and an attribute value. The system suggests possible attributes, operators, and attribute values as you type, and displays error messages in red when an expression is invalid. You can combine attribute-value expressions using either **AND** or **OR** operators, but do not combine both operators in the same filter expression.

For example, the following filter expression filters on the **Utility name** and **Action name** attributes...

```
'Utility Name' = 'session-manager' and 'Action Name' = 'EXPIRY'
```

...and returns only log entries with the respective attribute values of **session-manager** and **EXPIRY**.

Note: When using the **=** filter operator, attribute names and attribute values are case-sensitive.

6

Do one of the following:

- Click **Save filter** to save the filter to the **Filter** menu for future use.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Click **Apply** to apply the filter to the log immediately. The filter expression is not saved.

End of steps

8.31 How do I apply or clear my advanced filters?

8.31.1 Purpose

You can apply previously-saved advanced filters to the event log, or clear a filter as needed.

8.31.2 Steps

1

Open Users and System Security.

2

Select **User activity logs** from the drop-down list on the toolbar.

The User activity logs list displays a list of user events over a specified time period (All available, by default).

3

On the User activity logs list, click **Add filter** and select an advanced filter from the menu.

The event log is reduced to display only events that match the filter. You can repeat this step to apply a different filter.

4

Click **Clear filter** to remove the filter from the log view.

End of steps

8.32 How do I modify my advanced filters?

8.32.1 Purpose

You can modify previously-saved advanced filters.

8.32.2 Steps

1

Open Users and System Security.

2

Select **User activity logs** from the drop-down list on the toolbar.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The User activity logs list displays a list of events over a specified time period (All available, by default).

3

On the User Activity Logs list, click **Add filter**, **Manage saved filter**. The Manage filters form opens.

4

To modify a filter, hover over the filter item in the list and click **More**, **Edit**. The filter opens in the Edit filter form.

5

Edit the filter expression as required and do one of the following:

- Click **Update filter** to save the filter changes for future use.
- Click **Apply** to apply the modified filter to the event log immediately. The changes to the filter expression are not saved.

6

If you want to delete a filter, hover over the filter item in the list and click **More**, **Delete**. Click **Ok** to confirm the deletion.

7

Click **Ok** to close the Saved Filters form.

END OF STEPS

8.33 How do I set the User Activity Log to auto-refresh?

8.33.1 Purpose

The **Auto-refresh** function continually updates the Activity Log GUI with the most recent system events. Auto-refresh is disabled by default in User activity logs.

8.33.2 Steps

1

Open Users and System Security.

2

Select **User activity logs** from the drop-down list on the toolbar.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

The **Auto-refresh** option is at the bottom-left corner of the User activity logs view. Consider the following when enabling Auto-refresh:

- **Auto-refresh on:** if you select an event item in the activity log when Auto-refresh is enabled, the event selection and associated information in the Info panel is cleared at the next auto-refresh. You must select the event again to re-display its information in the Info panel.

  If you want an item selection to remain static while you view it, turn off Auto-refresh.
- **Auto-refresh off:** with Auto-refresh disabled, the User Activity Log is only updated when you click **Refresh list**.

END OF STEPS

8.34 How do I set limits for log event retention?

8.34.1 Purpose

Use the Users and System Security Settings form to set the maximum retention period for log events, the maximum number of log events to be retained, and overflow settings for log events that exceed the maximum.

8.34.2 Steps

1

Open Users and System Security.

2

Click **More actions**, **Settings**.

3

In the Users and system security settings form, click **User activity logs**.

4

Set the maximum number of days that log events will be retained in the **Log retention period** field (minimum 30 days, maximum 365 days).

5

Set the maximum number of individual log events that can be retained during the retention period in the **Maximum number of logs** field (minimum 100000 events, maximum 10000000 events).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

When either of the **Log retention period** or **Maximum number of logs** settings is approached or reached, a certain percentage of the stored log events are purged from the database.

Configure overflow settings for log events that approach or exceed the maximum settings:

- **Warning threshold (%):** percentage of maximum settings at which a warning message is sent.
- **Warning purge amount (%):** percentage of total log events purged from the database when warning threshold is reached.
- **Critical threshold (%):** percentage of maximum settings at which a critical warning message is sent.
- **Critical purge amount (%):** percentage of total log events purged from the database when critical threshold is reached.

7

Save your changes and close the form.

END OF STEPS

8.35 How do I export activity log events?

8.35.1 Purpose

You can export activity logs to an external file for archival purposes. You can export the entire log contents, or only selected events.

8.35.2 Steps

1

Open Users and System Security.

2

Select **User activity logs** from the drop-down list on the toolbar.

The User activity logs list displays a list of user events over a specified time period (All available, by default).

3

On the User activity logs list, do one of the following:

- To export the entire activity log contents, click ⋮ **More actions**, **Export all** on the NSP banner.
- To export only selected log events, select the events you want to export and then click ⋮ **Table settings and actions**, **Export selected**, **cvs | xlsx | xml**.

A Save as form appears.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Specify a location to save the export file and click **Save**.

The exported log is saved as a .csv file in a .zip archive.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Network resource groups

8.36 What are group directories and resource groups?

8.36.1 Group directories and groups

Network resource group directories and resource groups are groupings of network equipment. Resource groups are associated with roles to grant NSP user access permissions to specific network resources. A resource group is a collection of network objects of the same type, and a group directory is a collection of resource groups.

Note: Network resource groups have no relationship with resource pools. The two have completely different functions in NSP.

You can configure the following types of resource groups:

- Network element resource groups
- Port resource groups
- LAG resource groups
- Service resource groups

8.37 Pathway: create group directories and resource groups

8.37.1 Purpose

A resource group is a logical set of network equipment or services, specified by user-defined inclusion filters. A resource group can belong to multiple group directories.

8.37.2 Steps

1

Create a group directory; see 8.38 “How do I create a group directory?” (p. 205).

2

Add new resource groups to the group directory; see 8.39 “How do I configure a resource group?” (p. 206).

END OF STEPS

8.38 How do I create a group directory?

8.38.1 Purpose

This procedure describes how to configure a group directory. After you create a specific type of group directory, you can add resource groups of the same type from within the group directory.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.38.2 Steps

1

Open Resource Groups.

2

In the upper left-hand corner of the GUI, select from the menu the type of group directory you want to configure:

- Network Element Group Directories
- Port Group Directories
- LAG Group Directories
- Service Group Directories

3

On the Group Directories list on the left-hand side of the GUI, click **+Add New Group Directory**.

4

In the Add Directory form, specify a name and description for the group directory.

5

Click **Ok**. An empty group directory is added to the Group Directories list.

To add a resource group to the group directory, see 8.39 “How do I configure a resource group?” (p. 205).

END OF STEPS

8.39 How do I configure a resource group?

8.39.1 Purpose

This procedure describes how to configure a resource group. You create a specific type of resource group from within a group directory of the same type.

Note: When associating groups in LAG Group Directories, you can add a group, but after closing the window, adding a group is no longer possible. As a workaround, refresh the window.

8.39.2 Steps

1

Open Resource Groups.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

In the upper left-hand corner of the GUI, select from the menu the type of group directory in which you want to configure a resource group:

- Network Element Group Directories
- Port Group Directories
- LAG Group Directories
- Service Group Directories

3

On the Group Directories list on the left-hand side of the GUI, expand the group directory to which you want to configure a resource group.

4

On the group directory list item, click ···**More**, **Add Group**

5

In the Create Group form, specify a name and description for the resource group.

6

Specify network resources for the group by configuring inclusion filters:

- Click **Filter**.

  In the Advanced filter form, type a filter expression in the **Filter Expression** field, starting with a resource attribute, followed by a Boolean operator and an attribute value. The system suggests possible attributes, operators, and attribute values as you type, and displays error messages in red when an expression is invalid. You can combine attribute-value expressions using AND and OR operators.

  You can also use the Expression Builder; select a **Filter Attribute**, followed by a **Filter Operator**, and a **Filter Value**. Then click **+Add**. The expression is added to the **Filter Expression** field.

  If you are creating a filter to include a large number of resources, it is better to specify an attribute with a range of values to include the resources. Specifying a large number of individual resource attribute values linked together with OR operators creates a complex inclusion filter that will burden system resources and possibly cause the import process to fail.

  Any IPv6 addresses in an advanced filter expression must be enclosed in single quotation marks (‘ ‘).

When you have finished configuring your filters, click **Apply Filter**.

The filter-included resources are listed in the Create Group form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Click **Submit** to save the group.

END OF STEPS

8.40 How do I associate a resource group with a group directory?

8.40.1 Purpose

Use this procedure to associate an existing resource group with a group directory. You associate a resource group with a group directory by copying the resource group from another group directory and pasting it to the first group directory.

8.40.2 Steps

1

Open Map Layout and Groups.

2

In the upper left-hand corner of the GUI, select from the menu the type of group directory to which you want to configure a resource group:

- Network Element Group Directories
- Port Group Directories
- LAG Group Directories
- Service Group Directories

3

On the Group Directories list on the left-hand side of the GUI, expand a group directory that contains the resource group you want to associate.

4

On the resource group you want to associate, click ⋮**More**, **Copy**.

5

Click on the group directory with which you want to associate the resource group and click ⋮**More**, **Paste**.

The resource group is listed under the newly-associated group directory.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8.41 How do I search for a management object?

8.41.1 Purpose

Use this procedure to search for an NE, service, group directory, resource group, or network resource object. The availability of search objects depends on which resource group context you are viewing: Network Element | Port | Lag | Service Group Directories.

8.41.2 Steps

1

Open Resource Groups.

2

Click **Search**.

3

Select any of the available object types from the menu. For example:

- Group name
- Group directory name
- Service - name, ID, type
- NE - name, management IP, system ID
- Port - port name, NE name, description, system address
- Lag - lag name, NE name, description, system address

4

Type a search string in the text field. The list populates with near matches as you type.

5

Click **Close**.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Kafka authorization

8.42 What is Kafka authorization?

8.42.1 External client access

Kafka authorization ensures that an external client can only access known Kafka topic IDs, and to ensure that the events that a client has access to align with the access control specified for the APIs that they use. Kafka authorization ensures that NSP data security can be enforced according to the policies of a customer's security organization, thereby lowering the risk of a security attack and avoiding the process required to obtain security exceptions to deploy NSP.

Kafka events include internal NSP functions that use events to drive system behaviour and external clients (e.g., OSSes), that use events to reflect the state of NSP resources within their own systems.

There are currently several types of topics on the Kafka bus:

- Internal topics that are not exposed to the external clients.
- External topics that are created through the Kafka notification service and are intended for the sole use of the authenticated client that subscribed to them.
- External topics that are created through the Kafka notification service and are intended for use by some other user or group of users, e.g., Telemetry.
- Permanent external topics that are provided by the YANG notification service that are well-known and intended for the use of all internal and external authenticated clients.

Port behavior with Kafka Authorization enabled:

- Internal topics are only visible and consumable via internal ports: 9392 for internal client access and 9292 for Multi-NIC secure access.
- On external ports (9192, 9193, 9194), internal topics are fully restricted: no **consume**, **list**, **describe**, or any other operations on internal topics.

Kafka authorization supports dynamic updates to NSP user access control configurations without requiring Kafka cluster restarts.

8.42.2 Considerations for NFM-P

In a single NIC deployment, NFM-P uses port 9192 by default to communicate with NSP. If Kafka authorization is enabled, NFM-P loses access to internal topics on port 9192. Therefore, when NFM-P is present in the system, Kafka authorization is supported only in Multi-NIC deployments. In this case, the internalClientAuth parameter must be set to true in the nsp-config.yml file, NFM-P must connect via the internal/Multi-NIC port (9292), and mTLS must be configured in the samconfig utility on NFM-P.

8.42.3 Use cases

This section presents configuration examples for NSP functions with Kafka authorization enabled.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Securing nsp-yang-model.change case 1

Single NIC or multiple NIC, Kafka authorization enabled, no client authentication.

Kafka parameter configuration in nsp-config.yml:

- internalClientAuth: false
- externalClientAuth: false
- enableAcls: true

No restrictions on nsp-yang-model.change topic. It will always be visible to all users (internal and external).

Securing nsp-yang-model.change case 2

Multiple NIC with NFMP, Kafka authorization enabled, internal & external authentication enabled

Kafka parameter configuration in nsp-config.yml:

- internalClientAuth: true
- externalClientAuth: true
- enableAcls: true

Access to nsp-yang topics would depend on whether Global Access Control is enabled or disabled. If Global Access Control is disabled, external users can still see/consume nsp-yang topics. If Global Access Control is enabled, external users are restricted according to Kafka ACLs and NSP Notification Services permission defined in Roles.

Securing telemetry topics case 1

Single NIC or multiple NIC, Kafka authorization enabled, no client authentication.

Kafka parameter configuration in nsp-config.yml:

- internalClientAuth: false
- externalClientAuth: false
- enableAcls: true

No restrictions on telemetry topic. It will always be visible to all users/clients (internal and external) regardless of who created the subscriptions topic.

Securing telemetry topics case 2

Multple NIC with NFM-P, Kafka authorization enabled, internal and external authentication enabled

Kafka parameter configuration in nsp-config.yml:

- internalClientAuth: true
- externalClientAuth: true
- enableAcls: true

Access to telemetry topics would depend on if Global Access control is enabled or disabled. If Global Access Control is disabled, external users may still see/consume telemetry topics If Global

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Access Control is enabled, external users are restricted according to Kafka ACLs and NSP Notification Services Permission defined in roles.

Securing subscription-based topics: enforcing subscriber-only access

Kafka parameter configuration in nsp-config.yml:

- internalClientAuth: true
- externalClientAuth: true
- enableAcls: true

Kafka ACLs enforce topic-level authorization and subscription topics are mapped to specific user identities.

External users can access only their own subscription topics, except for telemetry topics (full access). External users cannot access other users' topics but can access telemetry topics created by other users if the NSP Notification Service has Read/Read-Write permission.

User roles and access control for subscription-based topics

An administrative user has access to their own subscription topics, telemetry topics, and nsp-yang-notification topics. They cannot access other administrative or non-administrative users' topics. Their allowed operations are List, Describe, and Consume. They can perform GET, POST, and DEL operations on their own NBI subscriptions only.

A Read/Write user has access to their own subscription topics, telemetry topics, and nsp-yang-notification topics. They cannot access other administrative or non-administrative users' topics. Their allowed operations are List, Describe, and Consume. They can perform GET, POST, and DEL operations on their own NBI subscriptions only.

A Read user can view subscriptions created before RBAC enforcement. They have access to their own subscription topics, telemetry topics, and nsp-yang-notification topics. They cannot access other administrative or non-administrative users' topics. Their allowed operations are List, Describe, and Consume. They cannot perform POST or DEL operations on NBI subscriptions. They can only perform a GET operation on their own subscriptions.

8.43 How do I enable Kafka authorization?

8.43.1 Purpose

This procedure describes how to enable Kafka authorization rules in an NSP deployment. Kafka authorization is disabled by default.

8.43.2 Steps

1

Open a terminal session.

2

Log in as the root or NSP admin user on the NSP deployer VM.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Stop the NSP cluster; see 12.8 “How do I stop an NSP cluster?” (p. 371).

4

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

5

Go to the Kafka Configuration section and uncomment the enableAcls parameter line by removing the leading `#` character.

You must preserve the leading spaces in the line.

6

Change the parameter value from `false` to `true`.

7

Save and close the nsp-config.yml file.

8

Enter the following to start the NSP cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member: nspdeployerctl --ask-pass install --config --deploy

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster starts, and the configuration update is put into effect.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9 Classic management security

Securing NFM-P system access

9.1 What is NFM-P system security?

9.1.1 Password security

For increased security, it is recommended that you regularly change the passwords of the administrative user accounts on NFM-P components, as described in the following procedures:

- 11.2 “How do I change the nsp user password?” (p. 339)
- 9.2 “How do I change an NFM-P main database password in a standalone system?” (p. 215)
- 9.3 “How do I change an NFM-P main database password in a redundant system?” (p. 218)

9.2 How do I change an NFM-P main database password in a standalone system?

9.2.1 Purpose

Perform this procedure to change the password of a user associated with the main database in a standalone NFM-P system.

CAUTION

Service Disruption

The procedure requires a restart of the NFM-P main server, which is service-affecting.

It is strongly recommended that you perform this procedure only during a scheduled maintenance period.

Note: Before you perform the procedure, you must ensure that each main server, auxiliary server, and main database is running and operational.

You can use the procedure to change only one user password at a time. To change multiple user passwords, you must perform the procedure multiple times.

When you change a password on one station, the NFM-P automatically updates the password on all other NFM-P stations.

9.2.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4

Enter the following:

```
bash$ ./nmsserver.bash passwd ↵
```

The script prompts you for the current Oracle SYS user password.

5

Enter the password. The script validates the password, and then displays a list of user names like the following:

```
SAM Database Users:
- sys
- database_user (installation default is samuser)
Other Database Users:
- sqltxplain
- appqossys
- outln
- dip
- system
- exit
```

6

Enter a user name. The script prompts you for a password.

7

Enter the new password, which must:

- Be between 4 and 30 characters long
- Contain at least three of the following:
  - lower-case alphabetic character
  - upper-case alphabetic character
  - numeric character
  - special character, which is one of the following:
    # $ _
- Not contain four or more of the same character type in sequence
- Not be the same as the user name or the reverse user name
- Not contain a space character
- Differ by at least four characters from the current password

If the password is valid, the script prompts you to retype the password.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Enter the new password again. The following prompt is displayed:

```
WARNING: Changing passwords may cause instability to the NFM-P server
as well as the Oracle proxy on the database server.
Do you want to proceed (yes/no)?:
```

9

Enter yes ↵. The script displays status messages and then exits. If the status indicates a password change failure, contact technical support.

10

Record the password in a secure location.

11

Perform the following steps.

1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```
4. Enter the following to stop the main database:

   ```
   # systemctl stop nfmp-main-db.service ↵
   ```

12

Start the main database.

1. Return to the open console window on the main database station.
2. Enter the following:

   ```
   # systemctl start nfmp-main-db.service ↵
   ```
3. Enter the following:

   ```
   # systemctl start nfmp-oracle-proxy.service ↵
   ```

13

Restart the main server.

1. Navigate to the /opt/nsp/nfmp/server/nms/bin directory on the main server station.
2. Enter the following to restart the main server:

   ```
   bash$ ./nmsserver.bash force_restart ↵
   ```
3. Enter the following to display the server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

14

Close the open console windows.

END OF STEPS

9.3 How do I change an NFM-P main database password in a redundant system?

9.3.1 Purpose

Perform this procedure to change the password of a user associated with the main database in a redundant NFM-P system.

CAUTION

Service Disruption

The procedure requires a restart of each main server, which is service-affecting.

Perform the procedure only during a scheduled maintenance period.

Note: Before you perform the procedure, you must ensure that each main server, auxiliary server, and database is running and operational.

You can use the procedure to change only one user password at a time. To change multiple user passwords, you must perform the procedure multiple times.

When you change a password on one station, the NFM-P automatically updates the password on all other NFM-P stations.

9.3.2 Steps

1

Log in to the primary main server station as the nsp user.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3



CAUTION

Service Disruption

Contact technical support before you attempt to modify the nms-server.xml file.

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

If you are changing the Oracle SYS user or Oracle database user password, disable the automatic database failover function.

1. Navigate to the /opt/nsp/nfmp/server/nms/config directory.
2. Open the nms-server.xml file using a plain-text editor such as vi.
3. Locate the following parameter entry:

   `dbAutoFailOver=`*`value`*
4. Record the parameter value.
5. Edit the entry to read:

   `dbAutoFailOver="no"`
6. Save and close the nms-server.xml file.
7. Navigate to the /opt/nsp/nfmp/server/nms/bin directory.
8. Enter the following:

   `bash$ ./nmsserver.bash read_config` ↵

   The configuration change is applied, and automatic database failovers are disabled.

Note: Leave the console window open; it is required later in the procedure.

4

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

5

Enter the following:

`bash$ ./nmsserver.bash passwd` ↵

The script prompts you for the current Oracle SYS user password.

6

Enter the password. The script validates the password, and then displays a list of user names like the following

```
SAM Database Users:
- sys
- database_user (installation default is samuser)
Other Database Users:
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
- sqltxplain
- appqossys
- outln
- dip
- system
- exit
```

7

Enter a user name. The script prompts you for a password.

8

Enter the new password, which must:

- Be between 4 and 30 characters long
- Contain at least three of the following:
  - lower-case alphabetic character
  - upper-case alphabetic character
  - numeric character
  - special character, which is one of the following:
    # $ _
- Not contain four or more of the same character type in sequence
- Not be the same as the user name or the reverse user name
- Not contain a space character
- Differ by at least four characters from the current password

If the password is valid, the script prompts you to retype the password.

9

Enter the new password again. The following prompt is displayed:

```
WARNING: Changing passwords may cause instability to the NFM-P server
as well as the Oracle proxy on the database server.
Do you want to proceed (yes/no)?:
```

10

Enter yes ↵. The script displays status messages and then exits. If the status indicates a password change failure, contact technical support.

11

Record the password in a secure location.

12

If you are changing a password other than the SYS or Oracle database user password, go to Step 18.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13

Stop each main database; stop the standby first, and then the primary.

1. Log in to the database station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```

4. Enter the following:

   ```
   # systemctl stop nfmp-main-db.service ↵
   ```

Note: For convenience, leave the console window open; it is required later in the procedure.

14

Stop the standby main server.

1. Log in to the standby main server station as the nsp user.
2. Open a console window.
3. Navigate to the /opt/nsp/nfmp/server/nms/bin directory.
4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Note: For convenience, leave the console window open; it is required later in the procedure.

15

Start each main database; start the primary first, and then the standby.

1. Return to the open console window on the database station.
2. Enter the following:

   ```
   # systemctl start nfmp-main-db.service ↵
   ```

3. Enter the following:

   ```
   # systemctl start nfmp-oracle-proxy.service ↵
   ```

4. Close the console window.

16

Restart the primary main server.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Return to the open console window on the primary main server station.
2. Enter the following:

   ```
   bash$ ./nmsserver.bash force_restart ↲
   ```

   The primary main server restarts.
3. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

Note: For convenience, leave the console window open; it may be required later in the procedure.

17

Start the standby main server.

1. Return to the open console window on the standby main server station.
2. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↲
   ```
3. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.
4. Close the console window.
5. Log out of the standby main server station.

18

CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the file.

If the dbAutoFailOver value recorded in Step 3 is yes, re-enable the automatic database failover function.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Navigate to the /opt/nsp/nfmp/server/nms/config directory on the primary main server station.
2. Open the nms-server.xml file using a plain-text editor such as vi.
3. Locate the following parameter entry:

   ```
   dbAutoFailOver="no"
   ```
4. Edit the entry to read:

   ```
   dbAutoFailOver="yes"
   ```
5. Save and close the nms-server.xml file.
6. Navigate to the /opt/nsp/nfmp/server/nms/bin directory.
7. Enter the following:

   ```
   bash$ ./nmsserver.bash read_config ↲
   ```

   The configuration change is applied, and automatic database failovers are enabled.

19

Close the open console windows.

20

Log out of the primary main server station.

END OF STEPS

9.4 How do I update the supported NFM-P TLS versions and ciphers?

9.4.1 Purpose

CAUTION

Service Disruption

Updating the TLS version and cipher support requires a complete NFM-P system shutdown, which creates a network management outage.

Perform the procedure only during a scheduled maintenance period of sufficient duration with the guidance of technical support.

Outdated TLS versions or ciphers present a security risk. Perform this procedure to update the lists of supported TLS versions and ciphers in an NFM-P system.

Note: An NFM-P system upgrade replaces the current TLS version and cipher support settings with the defaults for the new release. After an upgrade, you may need to reconfigure the settings.

Note: You require the following user privileges:

- on each main and auxiliary server station — root, nsp

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- on each main database station — root, Oracle management user

Note: The Oracle management user and group names are specified during database installation; the default is ‘oracle’ in the ‘dba’ group.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp, Oracle management users

9.4.2 Steps

Prepare new cipher and TLS files

1

Log in to the standalone or primary NFM-P main server station as the nsp user.

2

Enter the following:

```
bash$ cd /opt/nsp/nfmp/server/nms/bin/security_management/ssl ↵
```

3

Enter the following to create the default cipher list file:

```
bash$ ./ciphers_and_tls_update.bash create -cdc default-ciphers-file ↵
```

4

Enter the following to create the default TLS list file:

```
bash$ ./ciphers_and_tls_update.bash create -cdt default-TLS-file ↵
```

5

Enter the following to copy the default ciphers file to a new file:

```
bash$ cp default-ciphers-file new_ciphers_file ↵
```

where *new_ciphers_file* is the name to assign to the new ciphers file

6

Open *new_ciphers_file* using a plain-text editor such as vi.

7

Edit the file to remove any unsupported ciphers.

8

Save and close the file.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Enter the following to copy the default TLS file to a new file:

```
bash$ cp default-TLS-file new_TLS_file ↵
```

where *new_TLS_file* is the name to assign to the new TLS file

10

Open *new_TLS_file* using a plain-text editor such as vi.

11

Edit the file to remove any unsupported TLS versions.

Note: You must not remove TLSv1.2.

12

Save and close the file.

Distribute files to system components

13

If the NFM-P system is redundant, distribute the required files to the standby main server station.

1. Log in to the standby main server station as the root user.
2. Enter the following:

   ```
   # cd /opt/nsp/nfmp/server/nms/bin/security_management/ssl ↵
   ```
3. Copy the following files from the primary main server station to the current directory:
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/*new_ciphers_file*
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/*new_TLS_file*

14

If the system includes one or more auxiliary servers, distribute the required files to each auxiliary server station.

1. Log in to the auxiliary server station as the root user.
2. Enter the following:

   ```
   # cd /opt/nsp/nfmp/auxserver/nms/bin/security_management/ssl ↵
   ```
3. Copy the following files from the standalone or primary main server station to the current directory:
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/*new_ciphers_file*
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/*new_TLS_file*
4. Enter the following:

   ```
   # chown nsp:nsp new_ciphers_file ↵
   ```
5. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# chown nsp:nsp new_TLS_file ↵
```

15

Distribute the required files to each main database station.

1. Log in to the main database station as the Oracle management user.
2. Enter the following:

   ```
   bash$ mkdir ~user/cipher_update ↵
   ```

   where *user* is the name of the Oracle management user
3. Enter the following to switch to the root user:

   ```
   # su ↵
   ```
4. Copy the following files from the standalone or primary main server station to the *~user*/cipher_update directory, where *user* is the name of the Oracle management user:
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/ciphers_and_tls_update.bash
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/*new_ciphers_file*
   - /opt/nsp/nfmp/server/nms/bin/security_management/ssl/*new_TLS_file*
5. Enter the following:

   ```
   # chown -R user:group ~user/cipher_update/ ↵
   ```

   where

   user is the Oracle management user name

   group is the Oracle management user group
6. Enter the following:

   ```
   # chmod a+x ~user/cipher_update/ciphers_and_tls_update.bash ↵
   ```

   where *user* is the Oracle management user name

Stop NFM-P system

16

Close the open client sessions.

1. Open an NFM-P GUI client using an account with security management privileges, such as admin.
2. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.
3. Click on the Sessions tab.
4. Click Search. The form lists the open GUI and XML API client sessions.
5. Identify the GUI session that you are using based on the value in the Client IP column.
6. Select all sessions except for the session that you are using.
7. Click Close Session.
8. Click Yes.
9. Click Search to refresh the list and verify that only the current session is open.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10. Close the NFM-P User Security - Security Management (Edit) form.
11. Close the GUI.

17

If the NFM-P system is redundant, stop the standby main server.

1. Log in to the standby main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash stop ↲
   ```

   The main server stops.

18

If the system includes one or more auxiliary servers, stop each auxiliary server.

1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstop ↲
   ```

   The auxiliary server stops.

19

Stop the standalone or primary main server.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash stop ↲
   ```

   The main server stops.

20

If the NFM-P system is redundant, stop the standby database proxy.

1. Log in to the standby database station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↲
   ```

   The database proxy stops.

21

Stop the standalone or primary database proxy.

1. Log in to the database station as the root user.
2. Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3. Enter the following:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```

   The database proxy stops.

Apply new cipher and TLS lists

22

Perform the following steps on each main database station to apply the new TLS configuration.

1. Log in as the Oracle management user.
2. Enter the following:

   ```
   bash$ cd ~/cipher_update ↵
   ```

3. Enter the following:

   Note: The -fo parameter is optional, and sets the cipher priority according to the order in the specified file. If the parameter is not included, the cipher priority is set to the default order.

   ```
   bash$ ./ciphers_and_tls_update.bash apply -c new_ciphers_file -t new_TLS_file -fo ↵
   ```

   where

   new_ciphers_file is the updated ciphers file

   new_TLS_file is the updated TLS file

   The script applies the new configuration, and backs up the previous configuration in the following file:

   ciphers_and_tls_backup.*timestamp*.tar.gz

23

Perform the following steps on each main server station to apply the new TLS configuration.

1. Log in as the nsp user.
2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin/security_management/ssl ↵
   ```

3. Enter the following:

   Note: The -fo parameter is optional, and sets the cipher priority according to the order in the specified file. If the parameter is not included, the cipher priority is set to the default order.

   ```
   bash$ ./ciphers_and_tls_update.bash apply -c new_ciphers_file -t new_TLS_file -fo ↵
   ```

   where

   new_ciphers_file is the updated ciphers file

   new_TLS_file is the updated TLS file

   The script applies the new configuration, and backs up the previous configuration in the following file:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

ciphers_and_tls_backup.*timestamp*.tar.gz

24

If the system includes one or more auxiliary servers, perform the following steps on each auxiliary server station to apply the new TLS configuration.

1. Log in as the nsp user.
2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/auxserver/nms/bin/security_management/ssl ↲
   ```

3. Enter the following:

   Note: The -fo parameter is optional, and sets the cipher priority according to the order in the specified file. If the parameter is not included, the cipher priority is set to the default order.

   ```
   bash$ ./ciphers_and_tls_update.bash apply -c new_ciphers_file -t
   new_TLS_file -fo ↲
   ```

   where

   new_ciphers_file is the updated ciphers file

   new_TLS_file is the updated TLS file

   The script applies the new configuration, and backs up the previous configuration in the following file:

   ciphers_and_tls_backup.*timestamp*.tar.gz

Start NFM-P system

25

Start the standalone or primary database proxy.

As the root user on the database station, enter the following:

```
# systemctl start nfmp-oracle-proxy.service ↲
```

The database proxy starts.

26

If the NFM-P system is redundant, start the standby database proxy.

As the root user on the standby database station, enter the following:

```
# systemctl start nfmp-oracle-proxy.service ↲
```

The database proxy starts.

27

Start the standalone or primary main server.

As the nsp user on the main server station, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash start ↲
```

The main server starts.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

28

If the NFM-P system is redundant, start the standby main server.

As the nsp user on the standby main server station, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash start ↵
```

The main server starts.

29

If the system includes one or more auxiliary servers, start each auxiliary server.

As the nsp user on the auxiliary server station, enter the following:

```
bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart ↵
```

The auxiliary server starts.

30

Close the open console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P user security

9.5 What is NFM-P user security?

9.5.1 NFM-P user management scope

NSP Users and System Security, rather than the NFM-P, manages NFM-P GUI client access. To gain GUI client access, an NFM-P operator must sign in to the NSP UI.

Note: NFM-P user management is limited to NFM-P XML API client access; for such users, the NFM-P user group properties define the level of XML API access using the mechanisms described below.

9.5.2 User security mechanisms

This section describes the NFM-P user security mechanisms for providing and restricting access to various objects and functions. NFM-P user security includes the following:

- user group and account management, which involves the following elements:
  - "Scope of command roles" (p. 233) — contains the roles that define the level of user control in NFM-P functional areas such as the read, create, update, and delete access permissions
  - "Scope of command profiles" (p. 233) — contains the appropriate scope of command role for the types of tasks to be performed
  - 9.6.5 "Span of control" (p. 234) — list of objects to which a user has access
  - "Span of control profiles" (p. 235) — contains the required spans that allow group access to specific NFM-P objects
  - "Span rules" (p. 236) — directs the NFM-P to add new services to other spans in addition to the Default Service span
- global security parameters such as password expiry periods, the allowed number of login attempts, and any automated security e-mail notifications.
- managing user-group workspaces, which are customized configurations of NFM-P GUI elements; see "NFM-P custom workspaces" in the *NSP NFM-P Classic Management User Guide* for comprehensive workspace information
- monitoring and managing active client sessions
- deleting NFM-P security elements that are no longer required, such as inactive user accounts or user groups.
- configuring task monitoring parameters and monitoring the progress of operational tasks:
  - GUI client write operations initiated by clicking Apply or OK
  - all write operations performed via the XML API
  - some read operations; for example, when you click Resync or Collect All

Note: See Appendix B, "Classic management scope of command roles and permissions" for a list of the permissions, access levels, and descriptions of all predefined scope of command roles and profiles.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.6 How do I manage NFM-P user accounts and groups?

9.6.1 Introduction

You can create NFM-P user accounts and user groups to:

- provide access to the NFM-P functional areas that match operator requirements
- restrict access to functions or objects based on operator expertise or authority

Users have view access, read-write access, or no access to NFM-P objects and functions based on:

- the user group to which the user belongs
- the scope of command profile assigned to the user group

Functional defaults

The default NFM-P user account called admin is assigned the Administrator scope of command role and a span of control profile that has Edit Access assigned to each default span.

Note: Access Control is disabled by default. When Access Control is disabled, other NSP tools such as Sessions and User Activity Logs remain enabled and functional.

Note: To restrict user access to top-level functions such as NFM-P and NE security management, the following guidelines are recommended:

- Assign the administrator scope of command role to a minimal number of NFM-P user accounts.
- Assign each NFM-P user to a user group that has the minimum privileges for performing the required tasks.

9.6.2 General NFM-P security management rules

The following general rules apply to NFM-P user and group security management:

- Only database space limits the number of accounts and groups that can be created.
- A user cannot belong to more than one user group.
- Only one session per user account can be open at the same time on a client station.
- A scope of command profile allows user-group access to one or more NFM-P functional areas.
- A span of control profile allows user-group access to one or more NFM-P managed objects.
- A user group is associated with only one scope of command profile that can contain multiple scope of command roles.
- A user group is associated with only one span of control profile that can contain multiple spans.
- By default, a user group is assigned access to all NFM-P objects.
- A user acquires span of control access rights from the associated user group.
- When you modify a user group, and a user in the group has an open client session, client actions may fail for the user. To put the new user group permissions into effect, the user must close the current client session and open a new session.
- You can modify but not delete a span of control profile that is assigned to a group.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.6.3 Password management

An NFM-P user password must observe the following constraints:

- It must be 8 to 100 characters.
- It must contain at least three of the following character types:
  - lowercase
  - uppercase
  - special ()?~!@#$&*_+
  - numeric
- It cannot be the user name in forward or reverse order.
- It cannot include more than three consecutive instances of the same character.
- It must change according to a configurable schedule to prevent account lockout.
- It cannot be reused as a new password for the same user account.

9.6.4 Scope of command

A scope of command, which defines the actions that a user is allowed to perform, is a collection of configurable roles, which are sets of permissions. A scope of command profile contains one or more roles, and the profile is subsequently applied to a user group. Each user in the group acquires the access rights specified in the scope of command profile.

Scope of command roles

A scope of command role specifies the read, create, update, and delete access permissions for an NFM-P object type or functional area. You can create custom roles by assigning specific access permissions to different functional areas. The functional areas are organized in packages, methods, and classes. See Appendix B, “Classic management scope of command roles and permissions” for a list of all access permissions that can be assigned to a scope of command role.

Note: When you enable the Create permission, the Update permission is automatically enabled.

Note: When you enable the Update permission, the Create permission is not automatically enabled.

You can create an original scope of command role, or copy an existing role and modify the role permissions to create a role. The NFM-P has several predefined scope of command roles. See Appendix B, “Classic management scope of command roles and permissions” for a list of the permissions, access levels, and descriptions of all predefined scope of command roles and profiles.

Note: When you create a scope of command role, you must enable create, update/execute, and delete access to allow the modification of a class or package.

Scope of command profiles

A scope of command profile contains one or more scope of command roles, and is assigned to a user group. Each user in the group acquires the permissions from the scope of command roles in the profile.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.6.5 Span of control

The span of control for a user is a list of the objects over which the user has control, for example, a group of NEs or services. You can create an original span, or copy an existing span and modify the list of associated objects to create a new span. The objects that are in a span, or that can be added to a span, are called span objects.

The NFM-P has several predefined spans. Each new object, for example, a discovered NE, is added to the corresponding predefined span. Table 9-1, “predefined spans of control” (p. 233) lists the predefined spans and the type of span objects in each.

Note: You cannot modify or delete a predefined span.

Table 9-1 predefined spans of control

Span	Included objects
Default Topology Group Span	Topology groups
Default Router Span	Managed NEs
Default Script Span	CLI and XML API scripts, service templates, tunnel templates, and auto-provision profiles
Default Test Suite Span	Test suites
Default Group Span	Ring groups and VLAN groups
Default Bulk Operation Span	Bulk operations
Default Service Span	Services
Default Customer Span	Customers

Spans are specified in span of control profiles that are associated with user groups. A user can create an NFM-P object only when the predefined span for the object type is in the span of control profile. For example, if you do not have the Default Group Span in your span of control profile, you cannot create a ring group.

NEs are added automatically to a span when the parent topology group, ring group, or VLAN group is in a span. An object that is automatically added to a span cannot be removed from the span, but an explicitly added object can be removed.

Note: A user can view or configure a point-to-point connection only when each endpoint of the connection is in the user span of control. For example, when the endpoints of an LSP path are in different spans, you need view or configuration privileges in each span in order to view or configure the LSP path.

When you create a span, you can drag and drop NEs and topology groups into the span contents list.

Each user can control which objects the NFM-P displays in maps, lists, and navigation trees, based on the user span of control. The User Preferences form contains a parameter that globally specifies whether the Edit Access span objects of the user appear by default. Objects that are not in a View Access span of the user are not displayed, regardless of the user preference. See “To filter using span of control” in the *NSP NFM-P Classic Management User Guide* for information about configuring the user span of control display preference.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

In a list form, you can override the global display preference using the Span On parameter. The associated advanced filter form contains a selector for filtering the search results based on the span of control.

Span of control profiles



CAUTION

Service Disruption

It is recommended that you consider the effects of combining customer, service, and NE spans in a span of control profile.

For example, a user can modify a service only when the service, customer, and participating NEs are in one or more Edit Access spans of the user, and none of the objects is in a Blocked Edit or Blocked View span.

A span of control profile is a collection of one or more spans that is assigned to a user group. When you create a profile, each span in the profile is assigned one of the following access types:

- View Access—The user can view the span objects, unless the scope of command permissions deny read access.
- Edit Access—The user can modify the span objects, unless the scope of command permissions deny access.
- Blocked Edit—The user can view but not modify the span objects, regardless of the scope of command permissions.
- Blocked View—The user cannot view or modify the span objects, regardless of the scope of command permissions.

Blocked Edit and Blocked View spans restrict access to a subset of the objects in another span in the same profile. For example, when multiple span of control profiles each contain the Default Service Span, you can add a customer-specific Blocked View or Blocked Edit span to each profile so that the user group associated with a profile can view or configure only the services of specific customers.

A Blocked Edit or Blocked View span takes precedence over other spans. For example, when a user has an Edit Access span that contains all services and a Blocked View span that contains Customer A and Customer B, the user cannot view or configure the services that belong to Customer A and Customer B.

To ensure that span conflicts do not interfere with network troubleshooting, the NFM-P allows a user to execute tests on NEs and service sites that are not in an Edit Access span of the user. However, activities such as policy distribution, software upgrades, and statistics collection can be performed only by a user with Edit Access spans that contain the target objects.

CPAM span of control

CPAM topology maps support span of control for equipment group objects. There are no default CPAM spans. To allow movement of objects on CPAM maps, you must create a custom span of control for CPAM equipment groups and add it to the span of control profile for the required user

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

group. See “CPAM span of control” in the *NSP NFM-P Control Plane Assurance Manager User Guide*. CPAM topology maps are accessed under Tools → Route Analysis in the NFM-P main menu.

Span rules

By default, the NFM-P automatically adds a new service to the Default Service span. Using an XML API client, you can create policies called span rules that add new services to other spans in addition to the Default Service span.

A span rule is associated with a format or range policy, and applies to the users and user groups that are specified in the format or range policy. You can associate multiple range policies with one user and service type, which enables the automatic addition of a new service to a specific span based on the service ID specified when the service is created.

When you create a span rule, you must specify one of the following to indicate which spans receive the services that the user creates:

- the Edit Access spans of each user associated with the format or range policy
- each span that is explicitly named in the rule

The span rules associated with a format or range policy take effect for new services only when the format or range policy is administratively enabled and has a valid configuration that includes at least one user or user group.

See 9.8 “How do I configure sample span rule?” (p. 241) for a sample span rule configuration and implementation.

9.7 What is user activity logging?

9.7.1 Log records

The NFM-P logs each GUI and XML API user action, such as system access attempts and configuration changes in the main database. The following table lists the information in a user activity log record.

Table 9-2 User activity log record information

Field name	Description
Time	Time of activity
Session Type	Type of session, which is GUI, JMS, or XML API
Session ID	Client session identifier
Session IP Address	Client IP address
Session Time	Client session start time
Server IP Address	IP address of main server that reports the activity
Type	General activity type, which is Deployment, Operation, or Save

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 9-2 User activity log record information (continued)

Field name	Description
Sub Type	Specific activity type, which is Creation, Deletion, Modification, or name of the invoked method
Username	NFM-P username
Site Name	Name of affected NE, if applicable
Site ID	IP address of affected NE, if applicable
Object Name	Name of affected object
Object ID	Fully qualified name of affected object
Object Type	Type of affected object
State	Activity status, which is Failure, Success, or Timeout
Request ID	Identifier assigned to the request, which is unique to a session
Additional Info	Information such as old and new parameter values after a modification
XML	NFM-P object class descriptor, if applicable, and activity details in XML request format

To view general user activity log entries in the GUI, or retrieve the entries using the XML API, you require an NFM-P user account that has the Administrator or NFM-P Management and Operations scope of command role.

You can also enable the forwarding of user activity logs to a remote syslog server, as described in 9.7.2 “Remote syslog server forwarding” (p. 239).

Note: Viewing or retrieving LI user activity entries requires the Lawful Intercept Management role, and is restricted to the entries of users in the same LI user group.

The logged activity types are the following:

- Operation—a request for the NFM-P
- Deployment—a change that is deployed to an NE
- Save—a change to an object in the NFM-P database

Each user activity creates an Operation log entry. If the activity results in an NE configuration change, a Deployment entry is logged. If the deployed information differs from the information in the NFM-P database, a Save entry is logged. If appropriate, a log entry contains the activity details in XML format.

The following table lists the user activity types and describes the associated sub types.

Table 9-3 User activity types

Type	Sub Type	sub type description
Deployment	Creation	NE object creation
	Deletion	NE object deletion
	Modification	NE object modification

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 9-3 User activity types (continued)

Type	Sub Type	sub type description
Operation	*method*	Name of invoked method
Save	Creation	Database object creation
	Deletion	Database object deletion
	Modification	Database object modification

The User Activity form displays a filterable list of the logged user activities, and a filterable list of the logged client and server session activities. Client session activities include connection, disconnection, and access violation. Server session activities include startup and shutdown. The properties form of a client connection log record lists the activities performed by the user during the client session.

The client GUI allows direct navigation between the following objects:

- activity record and the associated session record
- activity record and the activity target object
- object properties form and the associated user activity list form
- NFM-P Task Manager task and the associated user activity list form
- session record and the associated user activity list form

The User Activity form lists the recent user session and activity entries; older entries are purged according to configurable storage criteria. See 21.11 “How do I set the NFM-P system preferences?” (p. 603) for information about configuring the user activity log retention criteria using the System Preferences form.

To archive user activity log entries before the entries are purged from the NFM-P database, an XML API client can use a time-based filter to retrieve entries from the sysact package using the find and findToFile methods. See “Inventory retrieval methods” in the Network Developer Portal for information about using the find and findToFile methods.

User activity logging is a valuable troubleshooting function. For example, if a port unexpectedly fails, you can quickly determine whether misconfiguration is the cause by doing one of the following:

- opening the port properties form and clicking User Activity to view the recent user activity associated with the port
- opening the User Activity form, filtering the list by object type or name, and then verifying the associated user activities

Note: Script execution is logged, but the actions that a script performs are not.

The following apply to user activity logging.

- A Deployment activity typically does not have an associated Save activity for the following reasons:
  - A Deployment activity takes place only after a successful Save activity, so a Deployment implies a Save.
  - A Save activity typically contains the same information as the associated Deployment activity.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- When a high-level object such as an NE is deleted, one aggregate activity record is created, rather than multiple NE child object activity records.
- The XML text in a log entry is limited to 4000 characters. If an activity generates more than 4000 characters of XML text, the text is truncated, and the truncation is indicated on the log entry form.

9.7.2 Remote syslog server forwarding

You can enable the forwarding of NFM-P user activity logs to a remote syslog server by specifying the target server parameters for **remote-syslog** using the NFM-P samconfig utility on a main server.

Each generated remote syslog message for user activity has the following fields:

- timestamp
- hostname of syslog producer
- program name
- User Activity Log message

The User Activity Log message is in JSON format, and includes the following:

User Activity Log syslog record example

The following is an example of an NFM-P User Activity Log record forwarded to a remote syslog server.

```
May 27 17:30:57 nfmp-mainserver-1 activitylogs: {"app":"NFM-P",
"clientHost":"203.0.113.7","reqMethod":"Save","addlParams":"{}",
"actionParams":[

],"respCodePhrase":"Success","timeStamp":"2020-05-27 17:30:56.330
+0530","affObjs":[

{"val":"securityManager","key":"fdn"}

,

{"val":"TSecurity Manager","key":"objectType"}

,

{"val":"0.0.0.0","key":"siteId"}

,

{"val":"0.0.0.0","key":"siteName"}

],"uid":"154","host":"203.0.113.7","action":"Modification","user":
"admin","reqURL":"N/A","respCode":"1"}
```

The fields in the example have the following values:

Note: In an NFM-P log record, the addlParams field is always empty, and the reqURL field always contains “N/A”.

- timestamp—May 27 17:30:57
- hostname of syslog entry producer—nfmp-mainserver-1

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- program name—activitylogs
- User Activity Log entry—remainder that begins with "app":"NFM-P"
  - app—function name from which action performed
  - clientHost—remote hostname or IP address that invokes action
  - reqMethod—type of action performed
  - actionParams—array; contains parameters passed to action
  - addlParams—array; contains parameters or other such values not in other fields; always empty in NFM-P record
  - respCodePhrase—human-readable action response code
  - timeStamp—time at which action completed
  - affObjs—array of affected-object attributes, for example, FDN and ID
  - uid—record ID
  - host—IP address of syslog entry producer
  - action—name of action performed
  - user—username under which action performed
  - reqURL—HTTP URL of the executed HTTP Request; always contains “N/A” in NFM-P record
  - respCode—action response code, in integer format

9.7.3 Client session control

Each GUI or XML API client request creates an NFM-P client session. You can view a list of the active client sessions on the Sessions tab of the NFM-P User Security - Security Management form. Using this form, an admin user, or a user with an assigned Security scope of command role, can also terminate one or more client sessions. When a GUI client session is terminated in this manner, each client GUI displays a warning message and the connection is closed after a short delay. See 9.35 “How do I view and manage the active GUI client sessions?” (p. 265) for more information.

Messaging connections

A list of active GUI connections and XML API JMS connections can be viewed on the Messaging Connections tab of the NFM-P User Security - Security Management form. Using this form, an admin user, or a user with an assigned Security scope of command role, can terminate one or more connections. When an XML API client connection is terminated, a notification is sent to the client, but the admin user must also remove the JMS client connection so that the server stops storing JMS messages for the session. See 9.36 “How do I disconnect an XML API JMS client connection or remove a durable subscription?” (p. 266) for more information.

Client delegate sessions

The threshold for the number of client sessions allowed on a client delegate server is configurable from the client GUI. When a user tries to open a client session that exceeds the threshold, the client delegate server opens the session, displays a warning message, and generates an alarm. The threshold-crossing function can help to balance the session load across multiple client delegate servers. You need the Update user permission on the Server package to configure the threshold. See 9.40 “How do I configure the number of allowed client sessions for a client delegate server?” (p. 270) for more information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.8 How do I configure sample span rule?

9.8.1 Overview

This section describes the configuration of a policy that instructs the NFM-P to automatically add each service created for a specific customer to an Edit Access span associated with the creator of the service. Only the service administrator for the customer can create or edit the specific customer services. In contrast, a typical service user can only view the specific customer services. The following table describes the tasks to configure a span rule.

Table 9-4 Sample span rule configuration

Task	Description
1. Create a span that contains the existing customer services.	• Choose Administration→Security→NFM-P User Security from the NFM-P main menu. • Choose Create→Span on the Span of Control tab. • Specify a span name for the customer services. • Use the Contents tab to specify the customer X services.
2. Create a span of control profile for the service administrator.	• Choose Administration→Security→NFM-P User Security from the NFM-P main menu. • Choose Create→Profile on the Span of Control tab. • Add the Default Service Span as a View Access span to the span of control profile, which allows the user to create a service. • Add the customer services span as an Edit Access span to the span of control profile.
3. Create a range policy for each service type that the service administrator for the customer can create. In the sample, the services are IES and VPRN.	• Choose Administration→Format and Range from the NFM-P main menu. • Choose Create→Range Policy. • Specify IES Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Click Add on the Users tab to assign the policy to the service administrator. • Choose Create→Range Policy. • Specify VPRN Service as the Object Type. • Specify Service ID as the Property Name. • Configure a range. • Click Add on the Users tab to assign the policy to the service administrator.
4. Create a span rule that contains the customer span.	• Choose Administration→Span Rules from the NFM-P main menu. • Specify a name for the customer span rule. • Set the Created In parameter to All listed spans. • Add the customer span on the Spans tab.

After the span rule is created, the service administrator creates a new VPRN service for the customer. The NFM-P uses the VPRN range policy to automatically configure the service ID, and applies the associated customer span rule when the service is saved. As a result, the service is added to the customer span and to the Default Service Span. The service administrator has Edit Access to the customer span, and, therefore, can modify the service, as required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.9 Pathway: configure and manage NFM-P user security

9.9.1 Stages

1

Assess the requirements for user access to the different NFM-P functional areas and develop a strategy for implementing user security. See 9.6 “How do I manage NFM-P user accounts and groups?” (p. 232) for more information.

2

Reserve a client GUI session for the admin user to ensure that the admin user can always log in; see 9.10 “How do I reserve an admin account login?” (p. 244) .

3

Create scope of command roles or modify the default role to meet your operational requirements; see 9.11 “How do I create a scope of command role?” (p. 245) .

4

Create scope of command profiles that contain the appropriate scope of command roles for the types of tasks to be performed; see 9.12 “How do I create a scope of command profile?” (p. 246) .

5

Create spans or modify the default span to meet your operational requirements. Add managed objects to the spans; see 9.13 “How do I create a span of control?” (p. 247) .

6

Create span of control profiles that contain the required spans; see 9.14 “How do I create a span of control profile?” (p. 248) .

7

Create span rules, as required, to automatically assign new services to spans other than the Default Service Span; see 9.15 “How do I create a span rule?” (p. 248) .

8

Manage user group security requirements, as required.

- Create or modify user groups and assign scope of command and span of control profiles to each group, as required; see 9.16 “How do I create an NFM-P user group?” (p. 249) .
- Add workspaces to user groups; see 9.17 “How do I add or remove workspaces for a user group?” (p. 250) .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Create, modify, or copy user accounts for performing the tasks that are associated with each user group; see 9.18 “How do I create an NFM-P user account?” (p. 252) and 9.19 “How do I copy an NFM-P user account?” (p. 253) .

10

Configure global user account parameters, as required.

- user-account expiry periods, password criteria, and a GUI inactivity timeout; see 9.20 “How do I configure global user account and password expiry?” (p. 254) and 9.21 “How do I configure the GUI client inactivity timeout?” (p. 255) .
- minimum username length; see 9.22 “How do I configure the minimum allowable user name length?” (p. 255) .
- allowed number of authentication attempts; see 9.23 “How do I configure authentication failure actions?” (p. 256) .
- suspended account actions; see 9.24 “How do I configure suspended account actions?” (p. 256) .
- automated e-mail notification; see 9.25 “How do I configure automated E-mail notification?” (p. 257) .

11

Configure global user activity logging, as required; see 21.11 “How do I set the NFM-P system preferences?” (p. 603) .

12

Manage local user accounts, as required.

- List inactive user accounts; see 9.26 “How do I list inactive user accounts?” (p. 258) .
- Suspend or reinstate user accounts; see 9.27 “How do I suspend or reinstate an NFM-P user account?” (p. 258) .
- Manage passwords.
  - As administrator, change the password of an NFM-P user account; see 9.28 “How do I change an NFM-P user password?” (p. 259) .
  - Force a specified NFM-P user to change the account password during the next login attempt; see 9.30 “How do I disable an NFM-P user password?” (p. 261) .
  - Change the account password of the current user; see 9.31 “How do I change the password of the current NFM-P user?” (p. 262) .
- Export user tab preferences; see 9.32 “How do I export the local tab preferences of one or more users?” (p. 262) .
- Assign user tab preferences; see 9.33 “How do I assign local tab preferences to users?” (p. 263) .

13

Monitor and manage the active client sessions, as required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Broadcast a message to one or more GUI operators; see 9.34 “How do I send a broadcast message to GUI clients?” (p. 264) .
- List and optionally close GUI client sessions; see 9.35 “How do I view and manage the active GUI client sessions?” (p. 265) .
- List and optionally close XML API client sessions; see 9.36 “How do I disconnect an XML API JMS client connection or remove a durable subscription?” (p. 266)
- View the NFM-P user activity logs to monitor GUI and XML API user activity; see 9.37 “How do I view the user activity log?” (p. 267) and 9.38 “How do I view the user activity associated with an object?” (p. 268) .

14

Configure or manage the following security functions, as required:

- Change the maximum number of concurrent NFM-P admin user sessions; see 9.39 “How do I change the maximum number of concurrent NFM-P admin operator positions?” (p. 269) .
- Limit the number of client sessions that the NFM-P accepts from one or more client delegate servers; see 9.40 “How do I configure the number of allowed client sessions for a client delegate server?” (p. 270) .

15

Change the default parameter setting for the Task Manager, as required; see 9.41 “How do I change the NFM-P Task Manager settings?” (p. 271) .

16

Export or import all workspaces and tab preferences, as required.

- Export all workspaces and tab preferences; see 9.42 “How do I export all workspaces and local tab preferences?” (p. 273) .
- Import all workspaces and tab preferences, import workspaces only, or import tabs only; see 9.43 “How do I import workspaces and local tab preferences?” (p. 273) .

9.10 How do I reserve an admin account login?

9.10.1 Purpose

You can reserve one client GUI session for administrative users only. This allows an administrator to manage the existing client GUI sessions. You must have an account with an assigned Security scope of command role to perform this procedure.

9.10.2 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Configure the Reserve Administrator Login parameter.

3

Save your changes and close the form.

4

Log in as required.

END OF STEPS

9.11 How do I create a scope of command role?

9.11.1 Purpose

You can create a set of user permissions that define an operator role and apply one or more scope of command roles to a user group using a scope of command profile. You must have an account with an assigned Security scope of command role to perform this procedure.

Note: You cannot delete a predefined scope of command role.
You cannot delete a scope of command role that is assigned to a scope of command profile when the scope of command profile is assigned to a user group that contains users.
Refer to Appendix B, “Classic management scope of command roles and permissions” for a complete list of command profiles, roles, and permission information.

9.11.2 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Scope of Command tab.

3

Click Create and choose Role. The Role (Create) form opens.

4

Configure the required parameters.

5

Configure the permissions for the scope of command role:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Click on the Permissions tab. A list of the NFM-P packages, classes, and methods is displayed.
2. Select the required access permissions, which are displayed in the list column headings, for each package, class, or method that you need to assign to the scope of command role.

6

Save your changes and close the form.

END OF STEPS

9.12 How do I create a scope of command profile?

9.12.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Scope of Command tab.

3

Click Create and choose Profile. The Scope of Command Profile (Create) form opens.

4

Configure the required parameters.

5

Assign one or more scope of command roles to the profile:

1. Click on the Roles tab and click Add. The Select Role - Role form opens.
2. Select one or more roles and click OK.

   Note: You cannot delete a scope of command profile that is assigned to a user group that contains users.

6

Save your changes and close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.13 How do I create a span of control?

9.13.1 Purpose

You can specify a set of NFM-P objects in a span of control and the type of user access available for the objects. You can apply one or more spans to a user group using a span of control profile. You must have an account with an assigned Security scope of command role to perform this procedure.

Note: You cannot delete a span of control that is assigned to a user group that contains users.

9.13.2 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Span of Control tab.

3

Click Create and choose Span. The Span (Create) form opens.

4

Configure the required parameters.

5

Add one or more objects for user access:

1. Click on the Contents tab.
2. Click Add and choose an object type. The Select *(object_type)* form opens.
3. Select one or more objects and click OK.

6

Save your changes and close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.14 How do I create a span of control profile?

9.14.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Span of Control tab.

3

Click Create and choose Profile. The Span of Control Profile (Create) form opens.

4

Configure the required parameters.

5

Assign one or more spans to the profile:

1. Click on the Spans tab. The predefined spans are listed.
2. Click Add and choose an access type. The Select *access_type* Spans form opens.
3. Select one or more spans in the list and click OK.

   Note: You cannot delete a span of control profile that is assigned to a user group that contains users.

6

Save your changes and close the form.

END OF STEPS

9.15 How do I create a span rule?

9.15.1 Purpose

A span rule is a policy that specifies to which span of control profiles, in addition to the Default Service Span, a newly created service is automatically assigned. You must have an account with an assigned Security scope of command role to perform this procedure.

See 9.8 “How do I configure sample span rule?” (p. 241) for a sample span rule configuration and implementation.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.15.2 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Span Rules from the NFM-P main menu. The Span Rules form opens.

2

Click Create. The Service Creation Span Rule (Create) form opens.

3

Configure the required parameters.

4

Associate one or more spans with the rule:

1. Click on the Spans tab and click Add. The Select Span(s) form opens.
2. Select one or more spans in the list and click OK.

5

Associate one or more format or range policies with the rule:

1. Click on the Format and Range Policies tab and click Add. The Select Format or Range Policies form opens.
2. Select one or more policies in the list and click OK.

6

Save your changes and close the form.

END OF STEPS

9.16 How do I create an NFM-P user group?

9.16.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the User Groups tab and click Create. The User Group (Create) form opens.

3

Configure the required general parameters.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Enable and configure the Maximum User Group Operator Positions Allowed parameter to specify the maximum number of operator positions for the user group, where one operator position allows for one NFM-P non-web client session and one web client session for the user group.

5

Configure the parameters in the Expiry Periods panel.

6

If the user group is for remote XML API users, configure the required parameters in the Remote Users panel.

7

Select a scope of command profile in the Scope of Command panel.

8

Select a span of control profile in the Span of Control panel.

9

If you are modifying a user group, click on the Format and Range Policies tab. The Select Format or Range Policies form opens.

10

Select one or more policies and click OK.

Note: When you change the scope of command or span of control profiles of a group, the permissions of each user in the group are altered immediately when you click OK. You cannot delete a user group that contains users.

11

Save your changes and close the form.

12

If an active client session is affected by the user group modification, restart the client.

END OF STEPS

9.17 How do I add or remove workspaces for a user group?

9.17.1 Steps

An NFM-P administrator can use this procedure to set conditions so that either users cannot change the list of workspaces on their User Preferences form or users can add additional

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

workspaces to their workspace selector. To create or add new workspaces for a user group, see “NFM-P GUI custom workspace procedures” in the *NSP NFM-P Classic Management User Guide* for more information.

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the User Groups tab.

3

Click Create or choose a user group and click Properties. The User Group (Create|Edit) form opens.

4

To configure the Allow Mandatory Workspaces Only parameter in the Mandatory Workspaces panel, choose one of the followingl:

a. Select the Allow Mandatory Workspaces Only check box.

Note: If you select the Allow Mandatory Workspaces Only check box, the Add button on the User Preferences→Workspaces form is dimmed and the user cannot change the list of workspaces on their User Preferences form.
Any existing user-defined workspaces in the User Preferences form are deleted when the Allow Mandatory Workspaces Only check box is selected.
The user can change the order that the workspaces appear in the workspace selector and set any workspace as the default workspace.

b. Deselect the Allow Mandatory Workspaces Only check box.

Note: The user can add additional workspaces to their workspace selector by clicking Add in the User Preferences form. See “NFM-P GUI custom workspace procedures” in the *NSP NFM-P Classic Management User Guide* for more information.
The user can change the order that the workspaces appear in the workspace selector and set any workspace as the default workspace.

5

Add mandatory workspaces to a specific user group:

1. Click Add. The Add Workspace form opens.
2. Choose a workspace from the list and click OK. The Add Workspace form closes.

   Note: All mandatory workspaces that are added to the user group by the administrator appear in the User Preferences→Workspaces form and in the workspace selector drop-down for each user in the user group and cannot be deleted.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

To remove a workspace from the user group, choose a workspace in the Mandatory Workspaces panel and click Delete.

7

Click Move Up or Move Down to reorder the workspaces in the list. The workspace at the top of the list is the default workspace.

Note: You need a minimum of one workspace in the User Group.
If the last user workspace is deleted, the users default workspace in the User Preferences form is replaced by the user group default workspace.

8

Save your changes and close the form.

END OF STEPS

9.18 How do I create an NFM-P user account?

Note: If you want to delete an NFM-P user account, schedules associated with the user account are deleted only if the schedule is not associated with a scheduled task.

9.18.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab and click Create. The User (Create) form opens.

3

Configure the required general parameters.

4

Click Select and choose a user group.

5

If required, test the validity of the user e-mail address by clicking Test e-mail beside the e-mail Address parameter.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: Before you test the validity of the user address, ensure that the outgoing SMTP server and test message are configured. See 9.25 “How do I configure automated E-mail notification?” (p. 257) for information about configuring the outgoing server and test message.

6

Configure the parameters in the Password panel.

7

In the UI Session panel, configure the Maximum User Operator Positions Allowed parameter to specify the maximum number of operator positions for the user, where one operator position allows for one NFM-P non-web client session and one web client session for the user.

The value for the Maximum User Operator Positions Allowed parameter cannot be greater than the Maximum User Group Operator Positions Allowed parameter value of the user group to which the user belongs.

Note: When two or more sessions of the same type are registered from a user ID, two or more operator positions are consumed.

8

To enable XML API client access:

1. Configure the required parameters in the OSS Session panel.
2. To apply an alarm filter to control or limit the alarms that the NFM-P forwards to XML API clients over JMS, click Select in the OSS Session panel and choose an alarm filter. See 21.32 “How do I configure alarm filters for XML API clients?” (p. 634) for more information.

9

Configure the required parameters in the Client IP Address panel.

10

Save your changes and close the form.

END OF STEPS

9.19 How do I copy an NFM-P user account?

9.19.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click on the Users tab.

3

Choose a user and click Properties. The User *type_of_user*, Group *user_group* (Edit) form opens.

4

Click Copy. A User (Create) form opens for the second user.

5

Configure the required parameters. You must change the User Name parameter and configure the User Password and Confirm Password parameters.

6

Save your changes and close the form.

END OF STEPS

9.20 How do I configure global user account and password expiry?

9.20.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Configure the Password Reuse Cycle and Password History Duration (days) parameters.

3

Configure the required parameters in the Expiry Periods panel.

Note: If you set any of the parameters to 0, the corresponding expiry period check is disabled.
You can specify how long an account can remain dormant before the account is locked using the Account Expiry (days) parameter.
When a user attempts to log in with an expired password, the user account is suspended.
When a user updates their password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Save your changes and close the form.

END OF STEPS

9.21 How do I configure the GUI client inactivity timeout?

9.21.1 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Change the GUI inactivity check for all GUI clients.

1. Configure the Non-Web Client Timeout (minutes) parameter.
2. Click Apply.

3

Change the GUI inactivity check for all users in a user group:

1. Click on the User Groups tab. A list of user groups is displayed.
2. Choose a user group from the list and click Properties. The User Group *name* (Edit) form opens.
3. Enable the Non-Web Override Global Timeout parameter.
4. Configure the Non-Web Client Timeout (minutes) parameter.

4

Save your changes and close the form.

END OF STEPS

9.22 How do I configure the minimum allowable user name length?

9.22.1 Steps

The minimum number of characters for a user name length is one, and the maximum number of characters is 40.

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

In the User Name panel, check the Enable box.

3

Configure the Minimum User Name Length Allowed parameter.

4

Save your changes and close the form.

END OF STEPS

9.23 How do I configure authentication failure actions?

9.23.1 Purpose

You can specify an authentication message or a lockout for a user account that exceeds the configured number of login authentication attempts. Only non–admin accounts can be locked out. Admin accounts always have access.

9.23.2 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the E-mail tab and configure the required parameters in the Authentication Failure Actions panel.

If you set the Attempts before lockout parameter to 0, the lockout function is disabled.

3

Save your changes and close the form.

END OF STEPS

9.24 How do I configure suspended account actions?

9.24.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click on the E-mail tab.

3

Configure the parameters in the Suspended Account Actions panel.

4

Save your changes and close the form.

END OF STEPS

9.25 How do I configure automated E-mail notification?

9.25.1 Purpose

You can configure the NFM-P to automatically send E-mail messages to users and administrators; for example, when locking out a user account that exceeds the allowed number of authentication attempts.

9.25.2 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the E-mail tab.

3

Configure the required parameters in the Outgoing E-mail Server SMTP panel.

4

Configure the Test Message parameter.

5

Save your changes and close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.26 How do I list inactive user accounts?

9.26.1 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab.

3

Click Inactive User Search and perform one of the following:

a. Choose ≥90 Days.

b. Choose ≥180 Days.

c. Specify another period:

1. Choose Custom User Inactivity Period. The Custom User Inactivity Period form opens.
2. Configure the User inactive greater than or equal to parameter.

User accounts that have been inactive for a number of days that are greater than or equal to the specified value are listed on the NFM-P User Security - Security Management (Edit) form.

4

Save your changes and close the form.

END OF STEPS

9.27 How do I suspend or reinstate an NFM-P user account?

9.27.1 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab.

3

Select a user account and click Properties. The User *type_of_user* (Edit) form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Configure the User State parameter to suspend or reinstate the user account.

5

Save your changes and close the form.

END OF STEPS

9.28 How do I change an NFM-P user password?

9.28.1 Purpose

An NFM-P administrator uses the Security Management form to maintain user accounts. An NFM-P operator can change their password from a separate form. If an operator forgets a password, an administrator can change the password for the operator.

When a user attempts to log in with an expired password, the user account is suspended. When a user updates their password, the password expiry period is reset, and the new password again expires when the Password Expiry (days) parameter value is reached.

9.28.2 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab.

3

Select a user and click Properties. The User *type_of_user* (Edit) form opens.

4

Configure the User Password parameter and the Confirm Password parameter.

5

Save your changes and close the form.

6

If you are changing the password of the NFM-P admin user, you must update the password for NSP cluster access to the NFM-P XML API.

Perform 9.29 “How do I update NSP XML API user access details?” (p. 260).

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.29 How do I update NSP XML API user access details?

9.29.1 Purpose

Perform this procedure to update the NSP mediation secret for the user name and password to access the NFM-P XML API. The NFM-P user must have both admin and OSS management roles in NFM-P.

9.29.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer VM.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

4

Enter the following to update the user name:

```
# ./nspdeployerctl secret -n psaRestricted -s nsp-mdt-mediator-secret
-p XML_API_USERNAME update ↵
```

The following prompt is displayed:

```
Please enter the XML_API_USERNAME:
```

5

Enter the user name as plaintext.

The following prompt is displayed:

```
Please confirm the XML_API_USERNAME:
```

6

Re-enter the user name.

The user name is updated in the NSP mediator secret.

7

Enter the following to update the password:

```
# ./nspdeployerctl secret -n psaRestricted -s nsp-mdt-mediator-secret
-p XML_API_PASSWORD update ↵
```

The following prompt is displayed:

```
Please enter the XML_API_PASSWORD:
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Enter the password as plaintext.

The following prompt is displayed:

```
Please confirm the XML_API_PASSWORD:
```

9

Re-enter the password.

The password is updated in the NSP mediator secret.

10

Close the console window.

END OF STEPS

9.30 How do I disable an NFM-P user password?

9.30.1 Purpose

You can disable the password of a specific NFM-P user in order to block subsequent login attempts by forcing a password change.

Note: Disabling a user password may affect current user sessions. For example, if the user attempts to open the NFM-P client when the password is invalidated, the user may be directed back to the NSP sign-in page. The operation fails until a valid password is assigned to the user.

9.30.2 Steps

1

Open an NFM-P GUI client.

2

Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security - Security Management (Edit) form opens.

3

Click on the Users tab.

4

Select a user and click Properties. The User *username* (Edit) form opens.

5

Select the Force User Password Change parameter.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Save your changes and close the form.

The next login attempt by the user is blocked, and the following message is displayed to the operator:

```
Your account password has expired and must be changed.
```

The operator must request a password from an administrator.

Note: To enable a password that you assign, you must deselect the Force User Password Change parameter.

END OF STEPS

9.31 How do I change the password of the current NFM-P user?

9.31.1 Steps

1

Open an NFM-P GUI client.

2

Choose Administration→Security→Change Password from the main menu. The Password Change form opens.

3

Configure the parameters.

4

Save your changes and close the form.

END OF STEPS

9.32 How do I export the local tab preferences of one or more users?

9.32.1 Purpose

You can export the local tab preferences of single or multiple users to a specified directory. You can reuse these saved tab preferences settings by importing them later.

The exported settings are the local tab preferences saved for the selected users, not the custom tab preferences saved in a workspace. See “To configure tab preferences” in the *NSP NFM-P Classic Management User Guide* for information about saving tab preferences in a workspace.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.32.2 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab.

3

Choose one or more users from the list.

4

Click Tab Preferences and choose Export to export the selected user's local tab preferences to a specified directory. The Export Directory window opens.

5

Specify the export directory, or create a directory or folder, and click OK. The selected user's local tab preferences are exported to the specified directory.

6

Close the form.

END OF STEPS

9.33 How do I assign local tab preferences to users?

9.33.1 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab.

3

Choose one or more users from the list.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Click Tab Preferences and choose Assign to assign the tab preferences from the specified directory to the selected users. The Import Directory window opens. To export local tab preferences to a specified directory, see 9.32 “How do I export the local tab preferences of one or more users?” (p. 262) .

5

Navigate to the directory from which you need to assign a tab preference.

Note: Only a single user’s tab preferences can be in the specified directory or an error message appears.

6

Click Open and click Yes. The assigned tab preferences overwrite the local tab preferences of the selected users.

All affected users who currently have a client session opened, other than the client session where the assign has been initiated, receive a system-generated message informing them that the local tab preferences have been changed and they must restart the client, or risk losing the changes. A client operator can use the Reply function to reply to the message.

7

Close the forms.

END OF STEPS

9.34 How do I send a broadcast message to GUI clients?

9.34.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Sessions tab.

3

Select the required client session and click Text Message. The Text Message form opens.

4

Enter a message in the Text Message form and click Send.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Close the form.

End of steps

9.35 How do I view and manage the active GUI client sessions?

9.35.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Sessions tab.

3

Specify a filter to create a filtered list of GUI or XML API JMS client sessions and click Search. The active client sessions are listed.

4

Review the session information.

5

To close a GUI client session, select a session in the list and click Close Session.

Note: Closing an XML API session has additional dependencies; see 9.36 “How do I disconnect an XML API JMS client connection or remove a durable subscription?” (p. 266) for more information.

6

Close the form.

End of steps

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.36 How do I disconnect an XML API JMS client connection or remove a durable subscription?

9.36.1 Steps

1

Using an account with an assigned Security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Messaging Connections tab.

3

Specify a filter and click Search. A list of active XML API client connections opens.

4

Select a connection in the list and perform one of the following:

a. Click Close Connection to shut down the client connection.

b. Click Remove Connection to shut down the client connection and remove the durable subscription.

5

Click Yes. The action is performed.

If you choose Close Connection, the connection is terminated, but the NFM-P continues to store JMS messages for the session.

If you choose Remove Connection, the NFM-P stops storing the JMS messages for the session.

Note: When you remove a durable subscription, the XML API client can still attempt to connect to the XML API. You can prevent an XML API client from attempting to connect by suspending the XML API user account. See 9.27 “How do I suspend or reinstate an NFM-P user account?” (p. 258) for more information.

6

Close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.37 How do I view the user activity log?

9.37.1 Purpose

You can view user activity log entries associated with the following:

- a user
- a client session

Note: Viewing user activity records other than LI activity records requires a user account with an assigned Administrator or NFM-P Management and Operations scope of command role.

Note: Viewing LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope is restricted to the records of users in the same LI user group.

9.37.2 Steps

1

Choose Administration→Security→User Activity from the NFM-P main menu. The NFM-P User Activity form opens.

2

Perform one of the following:

a. View the activities performed during a specific client session:
   1. Configure the filter criteria, if required, and click Search. A list of session entries is displayed.

      Note: Only client session entries with a State value of Connected contain activity entries.
   2. Select the required session entry and click Properties. The Session form opens.
   3. Click on the Activity tab.
   4. Configure the filter criteria, if required, and click Search. A list of activity entries is displayed.

b. View the activities of a specific user.
   1. Click on the Activity tab.
   2. Specify the required username as the Username filter criterion and click Search. A list of user-specific entries is displayed.

3

Select an entry in the list and click Properties. The Activity form opens.

4

Review the general information, which matches the columnar information on the User Activity list form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Depending on the activity Type and Sub Type, the Additional Info panel contains detailed activity information. If required, expand the panel to review the information. The following information is listed:

- **Type Operation, all Sub Types:**
  - left pane—object hierarchy in tree form; each object is selectable
  - right pane—properties and values of selected object in left pane

    The Actions property, which is highlighted in yellow for an object creation or modification activity, has values that represent the actions associated with the activity, such as create and modify.
- **Type Deployment or Save, Sub Type Modification:**
  - Property Name column—list of modified parameters
  - New Value column—the parameter value set during the activity
  - Old Value column—the previous parameter value

6

If required, expand the XML panel to display more information about the activity. The panel displays the following information:

- Full Class Name—the NFM-P class descriptor of the affected object type
- Additional Info—the activity details in the form of an XML request

Note: The displayed Additional Info text is limited to 4000 characters. If an activity generates more than 4000 characters of XML text, for example, access interface creation, the Additional Info panel of the log entry contains a “truncated” object, and the XML text contains a closing <truncated/> tag.

7

To navigate directly to the object of the activity, click View Object. The object properties form opens.

Note: The View Object button is dimmed when there is no object associated with the activity, for example, a user login or logout operation.

8

View the activity information and close the form.

END OF STEPS

9.38 How do I view the user activity associated with an object?

9.38.1 Steps

Note: Viewing user activity records other than LI activity records requires a user account with an assigned Administrator or NFM-P Management and Operations scope of command role.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Viewing LI user activity records requires a user account with an assigned Lawful Interception Management scope of command role. The scope is restricted to the records of users in the same LI user group.

1

Open the required object properties form.

2

Click User Activity. The Activity form opens.

Note: The User Activity function is available only for objects that exist in the NFM-P database. For example, the function is not available on the User Preferences form, because the settings on the form are saved in the client or client delegate file system.

3

Review the activity entries as described in 9.37 “How do I view the user activity log?” (p. 267) and close the form.

END OF STEPS

9.39 How do I change the maximum number of concurrent NFM-P admin operator positions?

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

9.39.1 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Locate the section that begins with following XML tag:

```
<samsession
```

7

Edit the following line in the section:

```
max5620SAMAdminSessions="value"
```

where *value* is the maximum number of concurrent admin operator positions

8

Save and close the nms-server.xml file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```

The NFM-P puts the configuration change into effect.

10

Close the open console windows.

END OF STEPS

9.40 How do I configure the number of allowed client sessions for a client delegate server?

9.40.1 Steps

The NFM-P continues to accept new client sessions from a client delegate server after the allowed number of sessions is reached. The maximum number of sessions is used as a guide for balancing the client session load among multiple client delegate servers.

1

Using an account with Update permission on the Server package, choose Administration→System Information from the NFM-P main menu. The System Information form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click on the Client Delegate Servers tab.

3

Select a client delegate server and click Properties. The Client Delegate Server (Edit) form opens.

4

Configure the Maximum UI Sessions parameter.

5

Save your changes and close the form.

END OF STEPS

9.41 How do I change the NFM-P Task Manager settings?

Note: The Task Manager is operational with the default values.

9.41.1 Steps

1

Log in to the primary or standalone main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4



CAUTION

Service Disruption

Contact technical support before you attempt to modify the nms-server.xml file.

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Open the nms-server.xml file using a plain-text editor such as vi.

5

Find and configure the required parameters:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- maxNumRetainedTasks
- numTasksToPurgeWhenFull
- successfulTasksPurgeInterval
- failedTasksPurgeInterval

6

Save and close the nms-server.xml file.

7

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

8

Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts, and the configuration change takes effect.

9

Modify the client configuration, if required.

1. Log in to an NFM-P single-user client or client delegate server station.

   Note: If you log in to a RHEL client delegate server station, you must log in as the nsp user.

   Note: If you log in to a single-user client station, you must log in as the user who installed the client, or as a local administrator.
2. Open a console window.
3. Navigate to the client configuration directory, typically /opt/nsp/client/nms/config on RHEL, and C:\nsp\client\nms\config on Windows.
4. Open the nms-client.xml file using a text editor.
5. Configure the autoRefreshInterval parameter.
6. Save and close the nms-client.xml file.
7. Repeat Step 7 and Step 8 to restart the main server.

10

Close the console windows and form. See the *NSP NFM-P Classic Management User Guide* for information about using the NFM-PTask Manager.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9.42 How do I export all workspaces and local tab preferences?

9.42.1 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click Settings and choose Export All. The Export Directory window opens.

3

Specify the export directory, or create a directory or folder, and click Save. All the workspaces and local tab preferences are exported to the specified directory. If the directory exists, a dialog box appears.

4

Click Yes to overwrite all the workspaces and local tab preferences saved in the existing directory.

5

Close the form.

END OF STEPS

9.43 How do I import workspaces and local tab preferences?

9.43.1 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click Settings and choose Import. The Import Directory window opens.

3

Click on the drop-down menu and choose one of the following:

a. Import All (default)—to import all the workspaces and local tab preferences.

   If you choose this option, you can click on the Overwrite Existing Workspace(s) check box to allow overwriting of existing workspaces.

b. Import Workspaces Only—to import only workspaces from the specified directory.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If you choose this option, you can click on the Overwrite Existing Workspace(s) check box to allow overwriting of existing workspaces.

c. Import Tabs Only—to import only local tab preferences from the specified directory.

4

Click Open. A confirmation dialog box displays the number of workspaces and local tab preferences that will be imported from the specified directory.

5

Click Yes.

All users whose local tab preferences change and currently have a client session open, other than the client session where the import has been initiated, receive a message to inform them of the local tab preference change and that they must restart the client, or risk losing the changes.

The user can use the Reply function to reply to the message.

For all users who have their current workspace changed and currently have a client session opened, the workspace selector displays Workspace Out of Sync. Select the current workspace from the workspace selector drop-down menu to apply the modified settings.

6

Close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10 Classic management NE security

10.1 What is NFM-P NE security?

10.1.1 Access management



CAUTION

Service Disruption

The NFM-P cannot obtain a secret value from an NE during resynchronization. It is recommended that you use only the NFM-P to configure a shared authentication secret.

Do not configure a shared authentication secret directly on a managed NE using another interface, for example, a CLI, or the NFM-P cannot synchronize the security policy with the NE.

You can use the NFM-P to configure security for managed-device access that includes the following:

- device user accounts, profiles, and passwords
- RADIUS, TACACS+, and LDAP authentication for NFM-P user accounts
- MAFs
- CPM filters
- DoS protection
- DDoS protection
- X.509 authentication
- TCP enhanced authentication

10.1.2 General rules

An NFM-P site user profile specifies which CLI commands or command groups are permitted or denied on a managed device. A profile can be associated with multiple NFM-P user accounts, and each user account can have up to eight associated profiles.

The following general rules apply to NFM-P security management for devices.

- The authentication settings on a device override any settings distributed by the NFM-P. For example, if you use the NFM-P to configure a user account with SHA authentication, and then distribute the account to a device that uses MD5 authentication, the account authentication type changes to MD5.
- MAFs and CPM filters must be manually distributed to a managed device.
- An operator can limit the type of managed device access per user, for example, allowing FTP access, but denying console, Telnet, and SNMP access.
- A user profile is independent of a user account, and is not in effect until associated with a user account.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.2 What are RADIUS, TACACS+, and LDAP?

10.2.1 Overview

RADIUS is an access server AAA protocol. The protocol provides a standardized method of exchanging information between a RADIUS client, which is located on a device and managed by the NFM-P, and a RADIUS server, which is located externally from the device and the NFM-P.

RADIUS provides an extra layer of login security. The RADIUS client relays user account information to the RADIUS server, which authenticates the user and returns user privilege information. The information defines the device access of the user. For example, a user may not be allowed to FTP information to or from the device.

You can create device user accounts as a backup to RADIUS, TACACS+, or LDAP authentication. In the event that a RADIUS, TACACS+, or LDAP function fails, the device user account provides device access.

TACACS+ and LDAP provide functions that are similar to RADIUS functions.

Note: The NFM-P checks for reachability to a TACACS+ server using UDP port 49 to prevent long timeout issues. However, all subsequent communication with the server uses TCP port 49.

See the appropriate RADIUS, TACACS+, or LDAP documentation for information about authentication server installation, configuration, and management.

For TACACS+ users, you can specify the following in a user template that is read by the global TACACS+ policy:

- the type of permitted device access, for example, console, FTP, or both
- a home directory
- a login script to execute

10.2.2 Combined local and remote authentication

An organization may have an established TACACS+ or RADIUS authentication configuration. You can add NFM-P client GUI user accounts to an existing TACACS+ or RADIUS user base for local NFM-P authentication.

Consider the following:

- You can create an NFM-P user account that matches a TACACS+, RADIUS, or LDAP user account. For example, if the RADIUS user account is Jane, you can create an NFM-P user Jane.
- Remote users with usernames that don’t abide by the following rules may not work correctly. An NFM-P user name must begin with an alphanumeric character, and can:
  - be from 1 to 40 characters in length
  - include the following special characters: **- _ . @**
  - not include a space character
- An NFM-P user that is authenticated remotely can log in to the NFM-P using the RADIUS, TACACS+, or LDAP password.
- For local NFM-P user authentication, the account password must meet the NFM-P password requirements.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

For example, for a user called Jane:

- The RADIUS user name is Jane, and the password is accessforjane.
- The NFM-P user name is Jane and password is !LetJane1In.

When Jane is authenticated by RADIUS, she can log in to the NFM-P client by typing in Jane and accessforjane. If the RADIUS server was down, and she could not be authenticated remotely, to be authenticated locally Jane must log in to the NFM-P client by typing jane and !LetJane1In.

10.3 What is device SSH security?

10.3.1 NSP SSH algorithm support for mediation

The following SSH client cryptographic algorithms are deprecated by the NSP and disabled by default for classic management and model-driven mediation in the NSP:

- Cipher: arcfour256,arcfour128,3des-cbc,blowfish-cbc
- Key Exchange: diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1,diffie-hellman-group1-sha1 (classic management mediation only)
- MAC: hmac-md5,hmac-sha1-96,hmac-md5-96
- Host Key: ssh-dss

For compatibility with older devices, you can restore NFM-P support for the disabled algorithms, as described in 10.4 “How do I restore support for disabled NE SSH algorithms?” (p. 276).

Note: Restoring the disabled algorithms is not recommended, but may be required as an interim measure until the devices in your network support the newer SSH algorithms.

10.4 How do I restore support for disabled NE SSH algorithms?

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences that include service disruption.

Contact technical support before you attempt to modify the server configuration.

CAUTION

Security Risk

Restoring support for older SSH algorithms lowers the level of security in your network.

You must perform the procedure only as an interim measure until the devices in your network support the newer SSH algorithms, or as directed by technical support.

Note: You must perform the procedure on each main server in the NFM-P system.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: In a redundant system, you must perform the procedure on the standby main server station first.

10.4.1 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file, and store the file in a secure location on a station outside the management network.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Locate the section that begins and ends with following XML comment tags:

```
<!--<sshSecurity
      -->
```

7

Locate the section that immediately follows; the section begins and ends with following XML tags:

```
<sshSecurity
          />
```

8

Replace the two sections with the following:

Note: The content below may include line breaks inserted during the publishing of this guide. You must join the broken lines by removing any line breaks between quotation marks.

```
<!-- <sshSecurity
bypassIgnoreSshKeyMismatch="false"
cipherAlgorithms="chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,
aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
aes192-cbc,aes256-cbc,arcfour256,arcfour128,3des-cbc,blowfish-cbc"
kexAlgorithms="curve25519-sha256,curve25519-sha256@libssh.org,
curve448-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-
nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group18-
sha512,diffie-hellman-group17-sha512,diffie-hellman-group16-sha512,
diffie-hellman-group15-sha512,diffie-hellman-group14-sha256,diffie-
hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-
hellman-group1-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-
group14-sha1,diffie-hellman-group1-sha1"
macAlgorithms="hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
hmac-sha1,hmac-md5,hmac-sha1-96,hmac-md5-96"
signatureAlgorithms="ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-
sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,rsa-sha2-512-cert-
v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-ed25519,sk-ecdsa-sha2-
nistp256@openssh.com,sk-ssh-ed25519@openssh.com,rsa-sha2-512,rsa-sha2-
256,ssh-rsa,ssh-dss"
/>
-->
<sshSecurity
bypassIgnoreSshKeyMismatch="false"
cipherAlgorithms="chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,
aes256-ctr,aes128-gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,
aes192-cbc,aes256-cbc,arcfour256,arcfour128,3des-cbc,blowfish-cbc"
kexAlgorithms="curve25519-sha256,curve25519-sha256@libssh.org,
curve448-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-
nistp256,diffie-hellman-group-exchange-sha256,diffie-hellman-group18-
sha512,diffie-hellman-group17-sha512,diffie-hellman-group16-sha512,
diffie-hellman-group15-sha512,diffie-hellman-group14-sha256,diffie-
hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-
hellman-group1-sha1,diffie-hellman-group-exchange-sha1,diffie-hellman-
group14-sha1,diffie-hellman-group1-sha1"
macAlgorithms="hmac-sha2-256-etm@openssh.com,hmac-sha2-512-
etm@openssh.com,hmac-sha1-etm@openssh.com,hmac-sha2-256,hmac-sha2-512,
hmac-sha1,hmac-md5,hmac-sha1-96,hmac-md5-96"
signatureAlgorithms="ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-
sha2-nistp384-cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-
v01@openssh.com,ssh-ed25519-cert-v01@openssh.com,rsa-sha2-512-cert-
v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ecdsa-sha2-nistp256,
ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-ed25519,sk-ecdsa-sha2-
nistp256@openssh.com,sk-ssh-ed25519@openssh.com,rsa-sha2-512,rsa-sha2-
256,ssh-rsa,ssh-dss"
/>
```

9

Save and close the nms-server.xml file.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10

Enter the following to restart the main server:

Note: When you restart the primary main server in a redundant system, a server activity switch begins, and the standby main server restarts as the primary main server. If you want to restore the initial primary and standby roles, you must perform this step on the standby main server once again after the server initializes as the primary.

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash stop ↵
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash start ↵
```

11

Close the open console windows.

END OF STEPS

10.5 What are CPM filters and traffic management?

10.5.1 Overview

Device CPMs provide dedicated traffic management and queuing hardware to protect the control plane. You can use CPM filters to specify which types of traffic to accept or deny, and to allocate and rate-limit the shaping queues for traffic directed to the CPMs.

Note: The 7705 SAR does not support Queue filters or MAC CPM IP filters.
There is no partial distribution of CPM IP filter policies to a 7705 SAR. When you distribute a CPM IP Filter policy to a 7705 SAR, every entry, property, and value in the policy must be supported by the NE, or the policy distribution to the 7705 SAR is blocked.

10.5.2 Supported management functions

The NFM-P supports the following CPM traffic management functions:

- traffic classification using CPM filters
  - Packets going to the CPM are first classified by the IOM into forwarding classes before recognition by the CPM hardware. You can use CPM filters to further classify the packets using L3/L4 information, for example, destination IP, DSCP value, and TCP SYN/ACK.
- queue allocation
  - Queues 1 — 8 are the default queues, which cannot be modified or deleted; unclassified traffic is directed to the default queues.
  - Queues 9 — 32 are reserved for future use.
  - Queues 33 — 2000 are available for allocation.
  - Queues 2001 — 8000 are used for per-peer queuing.
- queue configuration
  - PIR
  - CIR
  - CBS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- MBS

10.6 What is DoS protection?

10.6.1 Overview

The NFM-P supports the use of DoS protection on network and access interfaces. To protect NEs from the high incoming packet rates that characterize DoS attacks, you can use the NFM-P to configure DoS protection for the following scenarios:

- the arrival of unprovisioned link-layer protocol packets that are received from CE devices in the core network
- the arrival of excessive subscriber control-plane packets on L2 or L3 access interfaces in aggregation networks
- the arrival of excessive Ethernet CFM frames on L2 and L3 access interfaces, SAPs, and SDP bindings, based on a combination of CFM OpCode and MEG-level values

DoS protection limits the number of packets that are received each second, and optionally logs a violation notification if a policy limit is exceeded. You can use the NE System Security form to view the violations for a specific NE.

10.6.2 DoS protection in the core network

DoS protection in the core network limits the number of link-layer protocol packets that each network interface on an NE accepts for protocols that are not enabled on the interface. The interface drops the excessive packets instead of queueing the packets for processing by the CPU.

You can configure global DoS protection on an NE using the NE System Security form. DoS protection controls the following for unprovisioned link-layer protocols:

- the packet arrival rate per source on each network interface
- the overall packet arrival rate per source on the NE
- whether an NE sends a notification trap if a policy limit is exceeded

An NE that supports DoS protection automatically applies default DoS protection parameters to each network and access interface. These defaults limit only the overall packet arrival rate and apply to all of the interfaces on the NE.

10.6.3 DoS protection policies in aggregation networks

In a subscriber aggregation network, an NE typically receives few control-plane packets from a specific subscriber. If one or more subscribers generate excessive control-plane traffic, DoS protection policies can help to ensure that NEs do not become overburdened by these unwanted packets.

You can configure DoS protection policies to control the following on network interfaces, VPLS L2 access interfaces, and IES and VPRN L3 access interfaces:

- the control-plane packet arrival rate per subscriber host
- the overall control-plane packet arrival rate for the interface
- whether an NE sends a notification trap if a policy limit is exceeded

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

An NE that supports DoS protection automatically assigns a default DoS protection policy to each network and access interface. This default policy limits only the overall packet arrival rate for the interface, and cannot be deleted or modified.

See 10.13 “How do I configure an NE DoS protection policy?” (p. 291) for information about creating or modifying a DoS protection policy and assigning the policy to one or more NEs, and the *NSP NFM-P Classic Management User Guide* for information about applying a policy to service interfaces.

10.7 What is DDoS protection?

10.7.1 Overview

DDoS protection extends DoS protection by controlling traffic destined for IOM or CPM CPUs on a per-SAP, per-protocol basis. A DDoS protection policy isolates protocols from each other and, at the same time, isolates subscribers so that attacks or misconfigurations affect only the source SAP or protocol.

Policers are used to enforce a traffic rate-limiting function. Rate limiting is configurable in packets per second or kb/s. Configurable burst tolerance allows extra full handshake attempts, as required by some protocols.

When a policer determines that a packet is non-conformant, it discards the packet or marks it as low-priority. Low-priority traffic is more likely to be discarded at a downstream queueing point if there is protocol congestion. Traffic marking is also useful for routing protocols, where an operator may need to offer all packets to the CPU, and only discard packets if the CPU cannot keep up. A policer can be mapped to one or more traffic protocols.

The following types of policer can be configured in a DDoS protection policy:

- static policers, which permanently instantiate enforcement policers on SAPs
- local monitoring policers, which dynamically instantiate enforcement policers on SAPs

A DDoS protection policy can be applied to a capture SAP or to an MSAP. A DDoS protection policy that is assigned to a capture SAP typically has higher traffic rate limiting values than a policy that is assigned to an MSAP.

There are two types of DDoS protection policies:

- Access-interface type
- Port type

A default port-type policy does not initially reside in the NFM-P, but is collected from a supporting NE during discovery synchronization. The port-type policy applies only for select port-based protocols, and is applied automatically to all ports when the policy is distributed to an NE that supports the port-type policy.

An access-interface type DDoS protection policy can be applied to the following objects:

- base router network interface other than a system or loopback interface
- VPRN network interface a loopback interface
- VPRN L3 access interface

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- VPRN group interface SAP
- IES L3 access interface
- IES group interface SAP
- VPLS L2 access interface
- I-VPLS I-L2 access interface
- MVPLS L2 access interface
- I-MVPLS I-L2 access interface
- VLL E-Pipe L2 access interface
- VLL I-Pipe L2 access interface

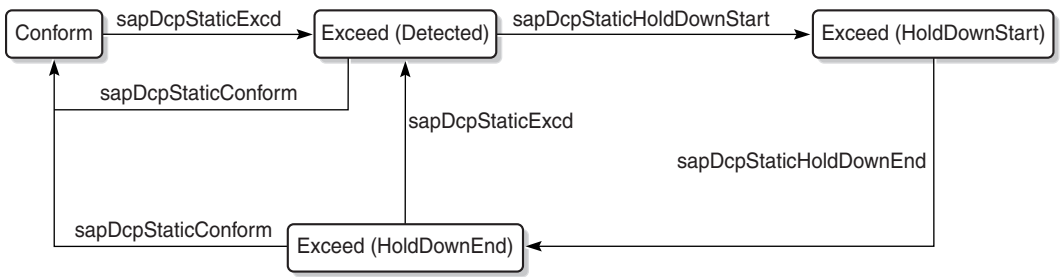
See 10.15 “How do I configure an NE DDoS protection policy?” (p. 293) for information about creating or modifying an NE DDoS protection policy and assigning the policy to one or more NEs.

10.7.2 DDoS alarm handling

To prevent raising multiple DDoS alarms against one affected object, the NFM-P raises one DDoS alarm per object, and updates the alarm as the object generates new DDoS events.

An operator can view dynamically updated alarm information, and avoid the generation of excessive numbers of individual DDoS alarm messages. Figure 10-1, “Static policer alarm message sequence” (p. 283) shows the alarm message sequence for a static policer. Figure 10-2, “Local monitoring policer alarm message sequence” (p. 284) shows the alarm message sequence for local monitoring policer. Figure 10-3, “Dynamic policer alarm message sequence” (p. 284) shows the alarm sequence for a dynamic policer. In each sequence, the alarm clears when the policer returns to the Conform state.

Figure 10-1 Static policer alarm message sequence



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 10-2 Local monitoring policer alarm message sequence

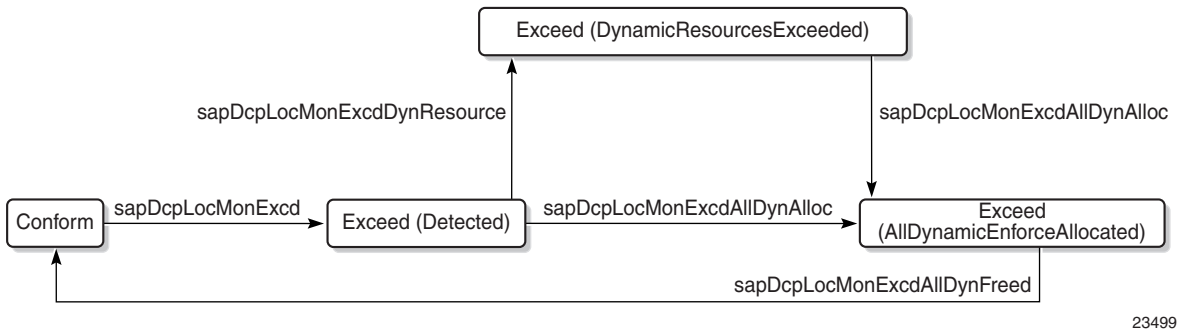
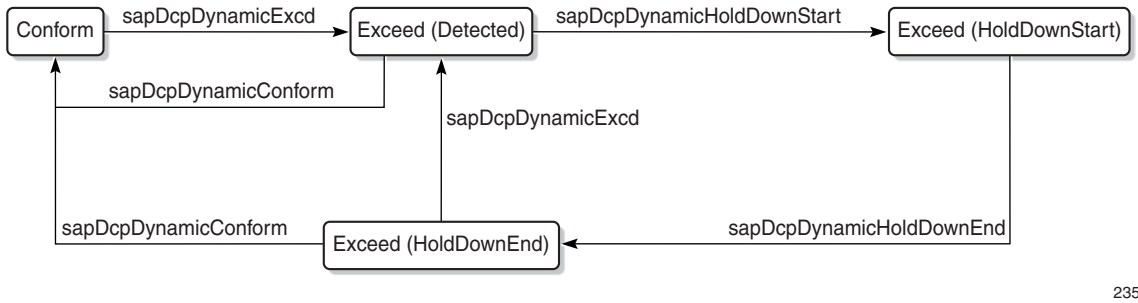


Figure 10-3 Dynamic policer alarm message sequence



10.8 What is IP security?

10.8.1 Overview

The NFM-P supports the IPsec MDA, which provides IP security support including tunneling and encryption functions. See the device security documentation for more information about configuring IP security.

10.9 HSM

10.9.1 Overview

The NFM-P supports the 1830 SMS netHSM security-key management platform.

To enable the 1830 SMS netHSM functions in the NFM-P, you must create an HSM configuration file on an NSP host server, and then enable and configure HSM on each main server. See the system installation procedures for information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.10 Pathway: manage NE user and device security

10.10.1 Stages

1

Specify the type of authentication keys used on the device; for example, SHA or MD5, as part of the device discovery. See “To commission a device for NFM-P management” in the *NSP NFM-P Classic Management User Guide* for more information.

2

Create a MAF for each device; see 10.11 “How do I configure a MAF?” (p. 287) .

3

Create filter policies for device CPM modules; see 10.12 “How do I configure a CPM filter?” (p. 288) .

4

Create NE DoS protection policies, as required to control the amount of subscriber-based control-plane traffic that the NE interfaces receive; see 10.13 “How do I configure an NE DoS protection policy?” (p. 291) .

5

View NE DoS protection violations, as required; see 10.14 “How do I view NE DoS protection violations?” (p. 292) .

6

Create NE DDoS protection policies, as required to isolate protocols from each other and isolate subscribers so that attacks or misconfigurations affect only the source SAP or protocol; see 10.15 “How do I configure an NE DDoS protection policy?” (p. 293) .

7

Configure NE TLS authentication for client NEs, as required; see 10.16 “How do I configure NE TLS client authentication?” (p. 295).

8

Configure NE TLS Authentication for servers, as required; see 10.17 “How do I configure NE TLS server authentication?” (p. 298).

9

Create site user profiles based on job classifications and the access needed to the managed devices; see 10.22 “How do I configure a site user profile?” (p. 302) .

10

Create individual site user accounts based on the configured profiles; see 10.23 “How do I

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

configure a user account on a managed device?” (p. 320) .

11

Specify password policies for access to managed devices and users; see 10.24 “How do I configure an NE password policy?” (p. 304) .

12

Create RADIUS, TACACS+, or LDAP access or security policies for user authentication on the managed device; see 10.25 “How do I configure an LDAP site authentication policy?” (p. 305), 10.26 “How do I configure an NE RADIUS authentication policy?” (p. 306), , 10.27 “How do I configure an NE TACACS+ authentication policy?” (p. 308) , or 10.28 “How do I configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy?” (p. 309) .

13

View or configure the system security settings on managed NEs; see 10.29 “How do I configure device system security settings?” (p. 310) .

14

As required, configure X.509 authentication or a PKI certificate authority profile; see 10.30 “How do I configure and manage PKI site security on an NE?” (p. 313) or 10.31 “How do I configure a PKI certificate authority profile?” (p. 316) .

15

Configure a PKI Enrolment over Secure Transport profile; see 10.34 “How do I configure an Enrollment over Secure Transport profile?” (p. 320).

16

Perform PKI CMPv2 actions, as required, to obtain or assign keys from a CA; see 10.37 “How do I perform CMPv2 actions?” (p. 322) .

17

Perform the following NE system security tasks, as required:

a. Delete security policies; see 10.38 “How do I delete a security policy?” (p. 325) .

b. Unlock user accounts that are locked due to failed login attempts; see 10.39 “How do I manually unlock a user account?” (p. 326) .

c. Clear the password history for a user on a managed object; see 10.40 “How do I clear the password history of a user on a managed device?” (p. 327) .

d. Perform CPMv2 certificate administration actions; see 10.37 “How do I perform CMPv2 actions?” (p. 322) .

e. Clear collected statistics information on a CPM filter; see 10.41 “How do I clear collected statistics on a CPM filter?” (p. 327) .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

f. Clear OCSP cache entries on an NE; see 10.42 “How do I manage OCSP cache entries on an NE?” (p. 329) .

10.11 How do I configure a MAF?

Note: To perform this procedure, you require an account with an assigned Administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

10.11.1 Steps

1

Choose Administration→Security→NE Management Access Filters from the NFM-P main menu. The NE Management Access Filter form opens.

2

Click Create or choose a policy and click Properties. The Site Management Access Filter (Create|Edit) form opens.

3

Configure the general parameters.

4

Configure the required parameters in the IPv4, IPv6, and MAC panels.

5

CAUTION

Service Disruption

When you set the Action parameter to deny, you cannot distribute the MAF to an NE.

You must set the parameter to permit, manually distribute the MAF as required, and then set the parameter to deny in each local MAF instance.

To configure an IPv4 or IPv6 entry, perform the following steps.

1. Click on the IPv4 Entries or IPv6 Entries tab.
2. Click Create or choose an entry and click Properties. The Site MAF Match Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Save your changes and close the form.

6

Repeat Step 5 to configure an additional IPv4 or IPv6 entry, if required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

To configure a MAC entry, perform the following steps.

1. Click on the MAC Entries tab.
2. Click Create or choose an entry and click Properties. The Site MAC Match Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click on the Filter Properties tab and configure the required parameters.

   If you set the Frame Type parameter to e802dot2LLC, configure the parameters in the Match Criteria - DSAP SSAP panel.

   If you set the Frame Type parameter to e802dot2SNAP, configure the parameters in the Match Criteria - SNAP panel.

   If you set the Frame Type parameter to Ethernet II, configure the Ether Type parameter.
5. Save your changes and close the form.

8

Repeat Step 7 to configure an additional MAC entry, if required.

9

Click Apply to save the changes.

10

Distribute the MAF to NEs, as required.

11

Close the open forms.

END OF STEPS

10.12 How do I configure a CPM filter?

Note: To perform this procedure, you require an account with an assigned Administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

The 7705 SAR does not support queue or MAC CPM filters.

10.12.1 Steps

1

Choose Administration→Security→NE CPM Filter from the NFM-P main menu. The NE CPM Filter form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click Create or choose a policy and click Properties. The CPM Filter (Create|Edit) form opens.

3

Configure the required parameters.

You can set the IP Administrative Status and IPv6 Administrative Status parameters to Up after you set the Scope parameter to cpm on the ACL IP and ACL IPv6 filter policies; see the *NSP NFM-P Classic Management User Guide*.

4

To configure an IPv4 filter entry, perform the following steps.

1. Click on the IPv4 Entries tab.
2. Click Create or choose an entry and click Properties. The CPM IP Filter Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click Select to assign a Log ID to the CPM filter entry.

   See the *NSP NFM-P Classic Management User Guide* for information on configuring a Filter Log policy that employs this Log ID.
5. Click on the Filter Properties tab.
6. Configure the required parameters.
7. Save your changes and close the form.

5

Repeat Step 4 to configure an additional IPv4 entry, if required.

6

To configure an IPv6 filter entry, perform the following steps.

1. Click on the IPv6 Entries tab.
2. Click Create or choose an entry and click Properties. The CPM IPv6 Filter Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click Select to assign a Log ID to the CPM filter entry.

   See the *NSP NFM-P Classic Management User Guide* for information on configuring a Filter Log policy that employs this Log ID.
5. Click on the Filter Properties tab.
6. Configure the required parameters.
7. Save your changes and close the form.

7

Repeat Step 6 to configure an additional IPv6 entry, if required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

To configure a MAC entry, perform the following steps.

1. Click Create or choose an entry and click Properties. The CPM MAC Filter Entry (Create|Edit) form opens.
2. Configure the required parameters.
3. Click Select to assign a Log ID to the CPM filter entry.

   See the *NSP NFM-P Classic Management User Guide* for information on configuring a Filter Log policy that employs this Log ID.
4. Click on the Filter Properties tab and configure the required parameters.

   If you set the Frame Type parameter to e802dot2LLC, configure the parameters in the Match Criteria - DSAP SSAP panel.

   If you set the Frame Type parameter to e802dot2SNAP, configure the parameters in the Match Criteria - SNAP panel.

   If you set the Frame Type parameter to Ethernet II, configure the Ether Type parameter.
5. Save your changes and close the form.

9

Repeat Step 8 to configure an additional MAC entry, if required.

10

To configure a queue entry, perform the following steps.

1. Click on the Queues tab.
2. Click Create or choose an entry and click Properties. The CPM Filter Queue Entry (Create|Edit) form opens.
3. Configure the required parameters.
4. Click on the CIR/PIR and Burst Size tab and configure the required parameters.

   Ensure that the Committed Burst Size (KB) parameter value is lower than the Maximum Burst Size (KB) parameter value.
5. Save your changes and close the form.

11

Repeat Step 10 to configure an additional queue entry, if required.

12

Click Apply to save the changes.

13

Distribute the filter to NEs, as required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14

Close the open forms.

END OF STEPS

10.13 How do I configure an NE DoS protection policy?

Note: To perform this procedure, you require an account with an assigned Administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

10.13.1 Steps

1

Choose Administration→Security→NE DoS Protection from the NFM-P main menu. The NE DoS Protection form opens.

2

Click Create or choose a policy and click Properties. The NE DoS Protection (Create|Edit) form opens.

3

Configure the required parameters.

4

Perform the following steps to configure CFM frame-rate limiting, if required.

1. Click on the CFM Rate Limiting tab.
2. Click Create. The CfmRateLimiting (Create) form opens.
3. Configure the required parameters:
4. Click Add in the Op Code Set panel. The Select Property form opens.

   Note: You must specify at least one Op Code value.
5. Choose one or more Op Codes in the list and click OK.
6. Save your changes and close the form.

5

Click Apply to save the changes.

6

Distribute the policy to NEs, as required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Close the open forms.

END OF STEPS

10.14 How do I view NE DoS protection violations?

10.14.1 Steps

1

Choose Administration→Security→NE System Security from the NFM-P main menu. The Select Site form opens.

2

Choose a managed device in the list and click OK. The NE System Security (Edit) form opens.

3

Click on the NE DoS Protection tab.

4

Perform one of the following to view a specific violation type.

a. Click on the Per MAC Source Violations tab to view a list of the violations associated with subscriber hosts according to MAC address.

b. Click on the Per IP Source Violations tab to view a list of the violations associated with subscriber hosts according to IP address.

c. Click on the Link Specific Port Violations tab to view a list of the violations at the port level. The following kinds of violations are listed:
   - violations that exceed the Link Rate Limit (pps) parameter value specified for the NE
   - violations that exceed the Port Overall Rate Limit (pps) parameter value specified for the NE.

d. Click on the Network Interface Violations tab to view a list of the violations for network interfaces that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

e. Click on the SAP Violations tab to view a list of the violations for SAPs that exceed the Overall Rate Limit (pps) parameter value specified in an associated NE DoS protection policy.

f. Click on the Video Router Context Violations tab to view a list of violations for virtual routers exceeding the per source limit on the NE.

g. Click on the Video Service Violations tab to view a list of violations for services exceeding the per source limit on the NE.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Repeat Step 4 as required to view another violation type.

6

Close the NE System Security (Edit) form.

END OF STEPS

10.15 How do I configure an NE DDoS protection policy?

10.15.1 Steps

1

Choose Administration→Security→NE DDoS Protection from the NFM-P main menu. The NE DDoS Protection form opens.

2

Click Create or choose a policy and click Properties. The DDoS Protection Policy (Create|Edit) form opens.

Note: For SAPs and access/network interfaces, click Search to list the default NE DDoS protection policies for Distributed CPU Protection (DCP). Select the appropriate access or network policy and click Properties to modify the default policy if required.

3

Configure the required parameters.

Note: A default port-type policy does not initially reside in the NFM-P, but is collected from a supporting NE during discovery synchronization. The port-type policy applies only for select port-based protocols, and is applied automatically to all ports when the policy is distributed to a supporting NE.

4

To configure a static policer, perform the following steps.

1. Click on the Static Policers tab.
2. Click Create or choose an entry and click Properties. The Static Policer (Create|Edit) form opens.
3. Configure the required parameters.
4. If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.
5. If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Time Limit (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6. Configure the Exceed Action parameter. If you set this parameter to Discard or Low Priority, configure the Hold Down Duration (seconds) parameter.
7. Click OK. The Static Policer form closes.

5

Repeat Step 4 to configure an additional static policer, if required.

6

To configure a local monitoring policer, perform the following steps.

1. Click on the Local Monitoring Policer tab.
2. Click Create or choose an entry and click Properties. The Local Monitoring Policer (Create|Edit) form opens.
3. Configure the required parameters.
4. If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.
5. If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Time Limit (seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.
6. Configure the Exceed Action parameter.
7. Click OK. The Local Monitoring Policer form closes.

7

Repeat Step 6 to configure an additional local monitoring policer, if required.

8

To configure protocol mappings for policers, perform the following steps.

1. Click on the Protocols tab.
2. Click Create or select an entry and click Properties. The Protocols (Create|Edit) form opens.
3. Configure the required parameters.
4. Select a policer in the Enforcement panel.

   Note: If the Type parameter is set to Static, you must choose a static policer. If the Type parameter is set to Shared, you must choose a shared policer. If the Type parameter is set to Dynamic, you must choose a local monitoring policer. However, if the Type parameter is set to Dynamic and the Local Monitoring Bypass parameter is enabled, you cannot specify a local monitoring policer.
5. If the Rate Type parameter is set to Kbps, configure the Rate Limit (Kb/s) and Buffer Space (Bytes) parameters in the Kbps panel. You can specify a default value for these parameters by selecting the Default check box.
6. If the Rate Type parameter is set to Packets, configure the Rate Limit (packets), Interval

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

(seconds), and Initial Delay (packets) parameters in the Packets panel. You can specify a default value for the Rate Limit (packets) parameter by selecting the Default check box.

7. Configure the Exceed Action parameter. If you set this parameter to Discard or Low Priority, configure the Hold Down Duration (seconds) parameter.
8. Save your changes and close the form.

9

Repeat Step 8 to configure an additional protocol, if required.

10

Click Apply to save the changes.

11

Distribute the policy to NEs, as required.

12

Close the open forms.

END OF STEPS

10.16 How do I configure NE TLS client authentication?

10.16.1 Purpose

This procedure describes TLS client configurations for NEs. For TLS server configurations, see 10.17 “How do I configure NE TLS server authentication?” (p. 298).

TLS configurations are distributed to NEs using the NFM-P policy framework; see “Policies overview” in the *NSP NFM-P Classic Management User Guide*.

10.16.2 Steps

1

Choose Administration→Security→NE TLS Authentication from the NFM-P main menu. The NE TLS Authentications form opens.

2

Configure a TLS client cipher list.

1. To create a new client cipher list, click Create→TLS Client Cipher List. The TLS Client Cipher List (Create|Edit) form opens.

   To modify an existing client cipher list, choose TLS Client Cipher List (NE Security) in the object drop down of the NE TLS Authentications form, click Search, select a cipher list, and click Properties.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. If you are creating a new cipher list, enter a name for the Client Cipher List in the General tab.
3. Click on the TLS Client Cipher List Param tab. You can configure up to eight parameter entries for the cipher list.
4. Click Create, or choose an entry in the list and click Properties. The TLS Client Cipher List Param form opens.
5. Configure the cipher list parameters.
6. Save your changes and close the form.
7. Click on the TLS 1.3 Client Cipher List Param tab. You can configure up to eight parameter entries for the cipher list.
8. Click Create, or choose an entry in the list and click Properties. The TLS 1.3 Client Cipher List Param form opens.
9. Configure the required parameters.
10. Save your changes and close the form.
11. Save your changes on the TLS Client Cipher List (Create|Edit) form and distribute the list to the required NEs.

3

Configure a TLS trust anchor profile.

1. To create a trust anchor profile, click Create→TLS Trust Anchor Profile. The TLS Trust Anchor Profile (Create|Edit) form opens.

   To modify a trust anchor profile, choose TLS Trust Anchor Profile (NE Security) in the object drop-down of the NE TLS Authentications form, click Search, select a trust anchor profile, and click Properties.
2. If you are creating a new profile, configure the Trust Anchor Profile Name on the General tab.
3. Click on the TLS Trust Anchors tab to add PKI certificate authority profiles.
4. Click Create, or choose a Trust Anchor CA Profile entry in the list and click Properties. The TLS Trust Anchor Entry form opens.
5. Select a Certificate Authority Profile. At least one PKI certificate authority profile must be selected; see 10.31 “How do I configure a PKI certificate authority profile?” (p. 316).
6. Save your changes and close the form.
7. Save your changes on the TLS Trust Anchor Profile (Create|Edit) form and distribute the profile to the required NEs.

4

Configure a TLS certificate profile.

1. To create a new TLS certificate profile, click Create→TLS Certificate Profile.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

To modify an existing certificate profile, choose TLS Certificate Profile (NE Security) in the object drop down of the NE TLS Authentications form, click Search, select a certificate profile, and click Properties.

The TLS Certificate Profile (Create|Edit) form opens.

2. If you are creating a new certificate profile, configure the Displayed Name parameter on the General tab.
3. Click on the TLS Certificate Profile Entry tab and configure the required parameters.
4. Click on the Send Chain tab to add the required PKI certificate authority profiles.
5. Click Create. The TLS Certificate CA Profile Entry form opens.
6. Select a Certificate Authority Profile; see 10.31 “How do I configure a PKI certificate authority profile?” (p. 316).
7. Save your changes and close the TLS Certificate CA Profile Entry form.
8. On the TLS Certificate Profile (Create|Edit) form, configure the Administrative State parameter if required.
9. Save your changes and distribute the list to the required NEs.

5

Note: The TLS client profile can be associated with a RADIUS server. For information, see 10.26 “How do I configure an NE RADIUS authentication policy?” (p. 306).

Configure a TLS client profile.

1. To create a new TLS client profile, click Create→TLS Client Profile. The TLS Client Profile (Create|Edit) form opens.

   To modify an existing client profile, choose TLS Client Profile (NE Security) in the object drop down of the NE TLS Authentications form, click Search, select a client profile, and click Properties.
2. If you are creating a new client profile, configure the Displayed Name parameter.
3. Select a Cipher List; see Step 2.
4. Select a Trust Anchor Profile; see Step 3.
5. Select a Certificate Profile; see Step 4 .
6. Select TLS client group list and TLS Client Signature List profiles.
7. Configure the required parameters.
8. Save your changes on the TLS Client Profile form and distribute the profile to the required NEs.

6

Close the NE TLS Authentications form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.17 How do I configure NE TLS server authentication?

10.17.1 Purpose

This procedure describes TLS server configurations for NEs. For TLS client configurations, see 10.16 “How do I configure NE TLS client authentication?” (p. 295).

TLS configurations are distributed to NEs using the NFM-P policy framework; see “Policies overview” in the *NSP NFM-P Classic Management User Guide*.

10.17.2 Steps

1

Choose Administration→Security→NE TLS Authentication from the NFM-P main menu. The NE TLS Authentications form opens.

2

Configure a TLS server cipher list.

1. To create a server cipher list, click Create→TLS Server Cipher List.

   To modify a server cipher list, choose TLS Server Cipher List (NE Security) in the object drop-down of the NE TLS Authentications form, click Search, select a cipher list, and click Properties.

   The TLS Server Cipher List (Create|Edit) form opens.
2. If you are creating a cipher list, configure the Displayed Name parameter on the General tab.
3. Click on the TLS Server Cipher List Param tab. You can configure up to 255 parameter entries for the cipher list.
4. Click Create, or choose an entry in the list and click Properties. The TLS Server Cipher List Param form opens.
5. Configure the required parameters.
6. Save your changes and close the TLS Server Cipher List Param form.
7. Click on the TLS 1.3 Server Cipher List Param tab. You can configure up to eight parameter entries for the cipher list.
8. Click Create, or choose an entry in the list and click Properties. The TLS 1.3 Server Cipher List Param form opens.
9. Configure the required parameters.
10. Save your changes and close the form.
11. Save your changes on the TLS Client Cipher List (Create|Edit) form and distribute the list to the required NEs.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Configure a TLS server profile.

1. To create a TLS server profile, click Create→TLS Server Profile.

   To modify a server profile, choose TLS Server Profile (NE Security) in the object drop-down of the NE TLS Authentications form, click Search, select a server profile, and click Properties.

   The TLS Server Profile (Create|Edit) form opens.
2. If you are creating a server profile, configure the Displayed Name parameter.
3. Select a Server Cipher List; see Step 2.
4. Select a Certificate Profile; see Step 4 in 10.16 “How do I configure NE TLS client authentication?” (p. 295).
5. Select a Trust Anchor Profile; see Step 3 in 10.16 “How do I configure NE TLS client authentication?” (p. 295).
6. Configure the Re-negotiate Timer parameter if required.
7. Select a Common Name List; see 10.33 “How do I configure a PKI common name list?” (p. 319).
8. Configure the required parameters.
9. Select TLS server signature list and TLS server group list profiles.
10. Save your changes on the TLS Server Profile form and distribute the profile to the required NEs.

4

Close the NE TLS Authentications form.

END OF STEPS

10.18 How do I configure TLS server group list?

10.18.1 Steps

1

Choose Administration→Security→NE TLS Authentication from the NFM-P main menu. The NE TLS Authentications form opens.

2

Click Create→TLS Server Group List. The TLS Server Group List, Global Policy (Create|Edit) form opens.

3

Configure the Displayed Name parameter on the General tab.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Click on the TLS 1.3 Server Group List Param tab.

1. Click Create, or choose an entry in the list and click Properties. The TLS 1.3 Server Group List Pararm, form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

5

Save your changes on the TLS Server Group List, Global Policy form and distribute the list to the required NEs.

END OF STEPS

10.19 How do I configure TLS client group list?

10.19.1 Steps

1

Choose Administration→Security→NE TLS Authentication from the NFM-P main menu. The NE TLS Authentications form opens.

2

Click Create→TLS Client Group List. The TLS Client Group List, Global Policy (Create|Edit) form opens.

3

Configure the Displayed Name parameter on the General tab.

4

Click on the TLS 1.3 Server Group List Param tab.

1. Click Create, or choose an entry in the list and click Properties. The TLS 1.3 Server Group List Pararm, form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

5

Save your changes on the TLS Client Group List, Global Policy form and distribute the list to the required NEs.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.20 How do I configure TLS server signature list?

10.20.1 Steps

1

Choose Administration→Security→NE TLS Authentication from the NFM-P main menu. The NE TLS Authentications form opens.

2

Click Create→TLS Server Signature List. The TLS Server Signature List, Global Policy (Create|Edit) form opens.

3

Configure the Displayed Name parameter on the General tab.

4

Click on the TLS 1.3 Server Group List Param tab.

1. Click Create, or choose an entry in the list and click Properties. The TLS 1.3 Server Group List Pararm, form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

5

Save your changes on the TLS Server Signature List, Global Policy form and distribute the list to the required NEs.

END OF STEPS

10.21 How do I configure TLS client signature list?

10.21.1 Steps

1

Choose Administration→Security→NE TLS Authentication from the NFM-P main menu. The NE TLS Authentications form opens.

2

Click Create→TLS Client Signature List. The TLS Client Signature List, Global Policy (Create|Edit) form opens.

3

Configure the Displayed Name parameter on the General tab.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Click on the TLS 1.3 Server Group List Param tab.

1. Click Create, or choose an entry in the list and click Properties. The TLS 1.3 Server Group List Pararm, form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

5

Save your changes on the TLS Client Signature List, Global Policy form and distribute the list to the required NEs.

END OF STEPS

10.22 How do I configure a site user profile?

Note: To perform this procedure, you require an account with an assigned Administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

10.22.1 Steps

1

Choose Administration→Security→NE User Profiles from the NFM-P main menu. The NE User Profiles form opens.

2

Click Create or choose a profile and click Properties. The Site User Profile (Create|Edit) form opens.

3

Configure the required parameters.

Note: You require LI user privileges to configure the LI Profile parameter.

4

Perform the following steps.

1. Click on the Entries tab.
2. Click Create or choose an entry and click Properties. The Site User Profile Match Entry (Create|Edit) form opens.
3. Configure the required parameters.

   The Match String parameter value is a CLI command prefix that defines the scope of the user profile. For example, when you set the match string to “config” and specify the deny action, the user profile cannot use any CLI commands that begin with the word “config”.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4. Save your changes and close the form.

5

Repeat Step 4 to configure an additional match entry, if required.

6

Click Apply to save the changes.

7

Distribute the profile to NEs, as required.

8

Close the open forms.

END OF STEPS

10.23 How do I configure a user account on a managed device?

Note: To perform this procedure, you require an account with an assigned Administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

10.23.1 Steps

1

Choose Administration→Security→NE User Configuration from the NFM-P main menu. The NE User Configuration form opens.

2

Click Create or choose a user and click Properties. The NE User (Create|Edit) form opens.

3

Configure the required parameters.

Note: The SNMP option of the Access parameter is not valid for NEs that are managed using SNMPv2.

4

If the Console option of the Access parameter is selected, perform the following steps to specify one or more site user profiles for the user account.

1. Click on the Console Profiles tab.
2. Use the Select buttons to specify up to eight profiles

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

When an SNMPv3 user account and group exist on a managed device, you can configure the user authentication parameters. To configure the parameters, perform the following steps.

Note: If MD5 or SHA authentication and DES or AES privacy is used, ensure that the keys are on the device and associated with the SNMPv3 user group.

1. Click on the SNMPv3 tab.
2. Configure the required parameters.

Note: Ensure the NEs support a valid combination of authentication and privacy protocols. See the NE documentation or *NSP NFM-P Classic Management User Guide* to review the disallowed combinations.

6

To specify an RSA key for use by SFTP on a 7750 SR MG, perform the following steps.

Note: Only the 7750 SR MG supports RSA key configuration.

1. Click on the RSA Key tab.
2. Click Create. The RSA Key (Create) form opens.
3. Configure the parameters.
4. Save your changes and close the form.

7

Click Apply to save the changes.

8

Distribute the account to NEs, as required.

9

Close the open forms.

END OF STEPS

10.24 How do I configure an NE password policy?

10.24.1 When to use

Perform this procedure to configure NE password parameters such as length, special characters, maximum attempts, expiry conditions, lockout time, and other site password policy considerations.

Note: To perform this procedure, you require an account with an assigned Administrator scope of command role to the sitesec package, or a scope of command role with write access permission to the sitesec package.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.24.2 Steps

1

Choose Administration→Security→NE Password Policy from the NFM-P main menu. The NE Password Policy form opens.

2

Click Create or choose an entry and click Properties. The Site Password Policy (Create|Edit) form opens.

3

Configure the required parameters.

4

Specify the types and order of password authentication to be used to verify the user account password using the Authentication Order 1 through 3 parameters. Set the order from the most preferred authentication method to the least preferred.

5

Configure the password complexity rules using the parameters in the Complexity Rules panel.

6

Click Apply to save the changes.

7

Distribute the policy to NEs, as required.

8

Close the open forms.

END OF STEPS

10.25 How do I configure an LDAP site authentication policy?

Note: Lightweight Directory Access Protocol (LDAP) is an authentication, authorization, and accounting (AAA) protocol. An LDAP AAA server stores and manages public keys. When a user needs to SSH to an NE SR-OS via a public key infrastructure, the SR NE obtains the key from the LDAP AAA server and authenticates the user with that key. An SR NE can only have one policy of this type.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.25.1 Steps

1

Choose Administration→Security→NE LDAP Authentication from the NFM-P main menu. The NE LDAP Authentication form opens.

2

Click Create or choose an entry and click Properties. The Site LDAP Policy (Create|Edit) form opens.

3

Configure the required parameters.

4

Click on the Servers tab.

5

Perform the following steps to specify a LDAP server:

1. Click Create or choose an entry and click Properties. The Site LDAP Server (Create | Edit) form opens.
2. Configure the required parameters.

   Note:

   Refer to 10.16 “How do I configure NE TLS client authentication?” (p. 295) for information regarding creation of NE TLS profiles.
3. Save your changes and close the form.

6

Click Apply to save the changes.

7

Distribute the policy to NEs, as required.

8

Close the forms.

END OF STEPS

10.26 How do I configure an NE RADIUS authentication policy?

Note: See the appropriate RADIUS documentation for information about configuring a RADIUS server.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.26.1 Steps

1

Choose Administration→Security→NE RADIUS Authentication from the NFM-P main menu. The NE RADIUS Authentication form opens.

2

Click Create or choose an entry and click Properties. The Site RADIUS Policy (Create|Edit) form opens.

3

Configure the required parameters.

4

Click on the Servers tab.

5

Perform the following steps to specify a RADIUS server.

Note: To associate a RADIUS server with a TLS client profile, see 10.16 “How do I configure NE TLS client authentication?” (p. 295).

1. Click Create or choose an entry and click Properties. The Site RADIUS Server (Create | Edit) form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

6

Repeat Step 5 to specify an additional RADIUS server, if required.

Note: You can specify up to five RADIUS servers.

7

Click Apply to save the changes.

8

Distribute the policy to NEs, as required.

9

Close the open forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.27 How do I configure an NE TACACS+ authentication policy?

Note: See the appropriate TACACS+ documentation for more information about configuring TACACS+ servers.

10.27.1 Steps

1

Choose Administration→Security→NE TACACS+ Authentication from the NFM-P main menu. The NE TACACS+ Authentication form opens.

2

Click Create or choose an entry and click Properties. The Site TACACS+ Policy (Create|Edit) form opens.

3

Configure the required parameters.

The Use Privilege Map parameter is configurable when the Enable Authorization parameter is set to true.

4

Click on the Privilege Level Map tab.

5

Click Create. The Privilege Level Map (Create) form opens.

6

Configure the Privilege Level parameter.

7

Choose a user profile.

8

Click on the Servers tab.

9

Perform the following steps to specify a TACACS+ server.

1. Click Create or choose an entry and click Properties. The Site TACACS+ Server (Create | Edit) form opens.
2. Configure the required parameters.
3. Save your changes and close the form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10

Repeat Step 9 to specify an additional TACACS+ server, if required.

Note: You can specify up to five TACACS+ servers.

11

Click Apply to save the changes.

12

Distribute the policy to NEs, as required.

13

Close the open forms.

END OF STEPS

10.28 How do I configure an OmniSwitch RADIUS, TACACS+, or LDAP security authentication policy?

10.28.1 Steps

1

Choose Administration→Security→NE AOS Security Authentication from the NFM-P main menu. The NE AOS Security Authentication form opens.

2

Click Create or choose an entry and click Properties. The Site AOS Security Policy (Create|Edit) form opens.

3

Configure the required parameters.

4

Click Apply to save the changes.

5

Distribute the policy to NEs, as required.

6

Close the open forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.29 How do I configure device system security settings?

10.29.1 Steps

1

Choose Administration→Security→NE System Security from the NFM-P main menu. The Select Site form opens.

2

Select a managed device and click OK. The NE System Security (Edit) form opens.

Note: Items that appear on the NE System Security (Edit) form are device-dependent. Not all configuration form tabs and parameters in this procedure apply to all devices.

3

To configure the FTP, Telnet, or SSH server parameters, click on the Servers Configuration tab.

Note: The 7705 SAR may become temporarily unreachable when enabling SSH and starting the SSH server on the device.

4

To configure allowed SSH ciphers, perform the following.

1. Click on the SSH Cipher List tab.
2. Click Create in the Client tab. The SSH Client Cipher List (Create) form opens.
3. Configure the required parameters.
4. Save and close the form.
5. Click on the Server tab and click Create. The SSH Server Cipher List (Create) form opens.
6. Configure the required parameters.
7. Save and close the form.

5

To configure SSH key regeneration, perform the following.

1. Click on the SSH Key Re Exchange tab.
2. Click on the Client tab and configure the required parameters.
3. Click on the Server tab and configure the required parameters.

6

To configure the CPM hardware queueing for BGP or T-LDP peers, click on the CPM Per-Peer-Queuing tab.

7

To configure user profiles, click on the System User Template tab. Otherwise, go to Step 20 .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The default System User radius_default and tacplus_default templates are listed.

8

Select the appropriate default template and click Properties. The System User Template (Edit) form opens.

9

Configure the required parameters.

10

If you intend to use the default Template Profile, go to Step 20 .

11

Click Select in the Template Profile panel to choose a template profile.

12

If you choose the administrative template, go to Step 20 .

13

Click Create. The Site User Profile (Create) form opens.

14

Configure the required parameters.

15

Click on the Entries tab.

16

Perform the following steps.

1. Click Create. The Site User Profile Match Entry (Create) form opens.
2. Configure the required parameters.

   The Match String parameter value is a CLI command prefix that defines the scope of the user profile. For example, when you set the match string to “config” and specify the deny action, the user profile cannot use any CLI commands that begin with the word “config”.

17

Repeat Step 16 to specify an additional match entry, if required.

18

Save your changes and close the form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

19

Close the System User Template (Edit) form.

20

To configure global DoS protection, click on the NE DoS Protection tab.

21

Configure the required parameters.

Note: PIM in an MVPN on the egress DR does not switch traffic from the (*,G) to the (S,G) tree if protocol protection is enabled, and if PIM is not enabled on the ingress network interface. Enable the Block PIM Tunneled parameter to enable extraction and processing of PIM packets that arrive from a tunnel, for example, an MPLS or GRE tunnel, on a network interface.

22

Click on the following child tabs, as required, to view the DoS violations.

- Per MAC Source Violations
- Per IP Source Violations
- Link Specific Port Violations
- Network Interface Violations
- SAP Violations
- SDP Violations
- Video Router Context Violations
- Video Service Violations

23

Click on the VPRN Network Exceptions tab to configure rate limits for VPRN network exceptions.

24

Configure the required parameters.

25

Save your changes and close the NE System Security (Edit) form.

26

Close the NE System Security form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.30 How do I configure and manage PKI site security on an NE?

10.30.1 Purpose

Perform this procedure to create the required DSA or RSA keypair and CA request on an NE to enable PKI security between peers, and to manage keys, certificates, and CRLs.

PKI encryption is required for functions such as IPsec, which use X.509 certificate-based authentication. The following devices support PKI encryption:

- 7450 ESS
- 7705 SAR
- 7750 SR MG
- 7750 SR
- 7750 SR
- 7705 SAR-Hm
- 7250 IXR

Note: The displayed parameters vary depending on the NE type, release, and the settings of other parameters.

10.30.2 Steps

1

Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the NFM-P main menu. The Select Site form opens.

2

Choose a managed NE and click OK. The Site Security Public Key Infrastructure (Edit) form opens.

3

Configure the required parameters.

4

Click Apply to save the changes.

5

Perform the following steps to generate a PKI keypair that is stored in a file on an NE compact flash drive.

1. Choose Admin Certificate→Generate Keypair from the More actions button menu. The Admin Certificate Generate Keypair form opens.
2. Configure the required parameters.
3. Click Execute. The keypair is generated and stored.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4. Close the form.

6

Perform the following steps to generate local PKCS#10 certificate request on a local compact flash drive.

1. Choose Admin Certificate→Generate Local Certificate Request from the More Actions button menu. The Admin Certificate Generate Local Certificate Request form opens.
2. Configure the required parameters.
3. Click Execute. The local request is generated.
4. Close the form.

7

If you want the certificate signed by a CA, FTP the request file to the CA and use the CA-signed certificate in the following steps.

8

Perform the following steps to convert the certificate file to the required format for the NE.

1. Choose Admin Certificate→Import File from the More Actions button menu. The Admin Certificate Import File form opens.
2. Configure the required parameters.
3. Click Execute. The file is imported.
4. Close the form.

9

To convert a certificate, keypair, or CRL file on the NE to another format, perform the following steps.

1. Choose Admin Certificate→Export File from the More Actions button menu. The Admin Certificate Export File form opens.
2. Configure the required parameters.
3. Click Execute. The file is exported.
4. Close the form.

10

To display the content of a certificate, keypair, or CRL file in plain text, perform the following steps.

1. Choose Admin Certificate→Display File from the More Actions button menu. The Admin Certificate Display File form opens.
2. Configure the required parameters.

   Note: If you are displaying key file content, only the Key Size and Key Type are displayed.

   Note: You must configure the Password parameter if the file uses PKCS#12 encryption.
3. Click Execute. The file content is displayed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4. Close the form.

11

To reload a certificate or keypair file from a local compact flash drive, perform the following steps.

1. Choose Admin Certificate→Reload File from the More Actions button menu. The Admin Certificate Reload File form opens.
2. Configure the required parameters.
3. Click Execute. The file content is reloaded.
4. Close the form.

12

To clear the OCSP cache, perform the following steps.

1. Choose Admin Certificate→Clear OCSP Cache from the More Actions button menu. The Admin Certificate Clear OCSP Cache form opens.
2. Configure the required parameters.
3. Click Execute. The file content is reloaded.
4. Close the form.

13

To import a Secure ND RSA keypair, perform the following steps.

1. Choose Admin Certificate→Secure ND Import from the More Actions button menu. The Admin Certificate Secure ND Import form opens.
2. Configure the required parameters.
3. Click Execute. The keypair is imported.
4. Close the form.

14

To export the Secure ND RSA keypair, perform the following steps.

1. Choose Admin Certificate→Secure ND Export from the More Actions button menu. The Admin Certificate Secure ND Export form opens.
2. Click Execute. The keypair is exported.
3. Close the form.

15

To perform CMP2 actions, see 10.37 “How do I perform CMPv2 actions?” (p. 322) .

16

To enroll EST profile, perform the following steps.

1. Choose Admin Certificate→Enroll EST Profile from the More Actions button menu. The Admin Certificate Enroll EST Profile form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Configure the required parameters.
3. Click Execute. The file content is enrolled.
4. Close the form.

17

To EST distribute CA Certificate, perform the following steps.

1. Choose Admin Certificate→EST Distribute CA Certificate from the More Actions button menu. The Admin Certificate EST Distribute CA Certificate form opens.
2. Configure the required parameters.
3. Click Execute. The file content is distributed.
4. Close the form.

18

To renew EST profile, perform the following steps.

1. Choose Admin Certificate→Renew EST Profile from the More Actions button menu. The Admin Certificate Renew EST Profile form opens.
2. Configure the required parameters.
3. Click Execute. The file content is renewed.
4. Close the form.

19

Close the Site Security Public Key Infrastructure (Edit) form.

END OF STEPS

10.31 How do I configure a PKI certificate authority profile?

10.31.1 Steps

Note: The displayed parameters vary depending on the NE type, release, and the settings of other parameters.

1

Choose Administration→Security→NE PKI Authentication→PKI Certificate Authority Profiles from the NFM-P main menu. The PKI Certificate Authority Profiles form opens.

2

Click Create. The Certificate Authority Profile (Create) form opens.

3

Configure the required parameters.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Click on the CMPv2 tab and configure the required parameters.

5

To create a CMP key, perform the following steps.

Note: A key that is created locally on an NE, for example, using a CLI, is not sent to the NFM-P, and is displayed on the Certificate Authority Profile form as N/A. Any N/A keys on an NE must be deleted before the profile can be distributed to the NE.

1. Click Create. The CMP Key List (Create) form opens.
2. Configure the parameters.
3. Save your changes and close the form.

6

To configure automatic CRL file download, perform the following.

1. Click on the Auto CRL Update tab and click Create. The Auto CRL Update form opens.
2. Configure the required parameters.
3. To specify a URL for the CRL file, click on the Create button in the URL entries panel and configure the parameters in the CRL URL Entry form. See 10.36 “How do I create a file transmission profile?” (p. 322) for information about creating a file transmission profile to use with the CRL URL entry.
4. Save your changes and close the form.

7

Click Apply to save your changes.

8

Distribute the policy to NEs, as required.

9

Close the open forms.

END OF STEPS

10.32 How do I configure the automatic renewal of the PKI certificate?

10.32.1 Automatic renewal

Before a PKI certificate expires, you can configure the automatic generation of a new CMP key and use an enrollment protocol (for example, CMPv2 or EST) to obtain a new certificate from the CA.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.32.2 Steps

1

Choose Administration→Security→NE PKI Authentication→PKI Certificate Authority Profiles from the NFM-P main menu. The PKI Certificate Authority Profiles form opens.

2

Click Create. The Certificate Authority Profile (Create) form opens.

3

Configure the required parameters.

4

Click on the CMPv2 tab.

5

Configure the required parameters and click OK.

6

Choose Administration→Security→NE PKI Authentication→Certificate Update Profile. The Certificate Update Profile form opens.

7

Click Create. The Certificate Update Profile, Global Policy (Create) form opens.

8

Configure the required parameters. Select the certificate authority profile that you created in Step 3 and click OK.

9

Choose Administration→Security→NE PKI Authentication→Certificate Auto Update Profile. The Certificate Auto Update Profile form opens.

10

Click Create. The Certificate Auto Update Profile, Global Policy (Create) form opens.

11

Configure the required parameters. Select the certificate update profile that you created in Step 8 and click OK.

12

Update and execute the admin certificate:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the NFM-P main menu. The Site Public Key Infrastructure form opens.
2. Choose an NE in the list and click OK. The Site Security Public Key Infrastructure (Edit) form opens.
3. Configure the required parameters.
4. Choose Admin Certificate→Update certificate. The Admin Certificate Update Certificate form opens.
5. Configure the certificate auto update profile that you created in Step 8.
6. Click Execute.

13

Close the forms.

END OF STEPS

10.33 How do I configure a PKI common name list?

Note: PKI configurations are distributed to NEs using the NFM-P policy framework; see "Policies overview" in the *NSP NFM-P Classic Management User Guide*.

10.33.1 Steps

1

Choose Administration→Security→NE PKI Authentication→PKI Common Name List from the NFM-P main menu. The PKI Common Name List form opens.

2

Click Create, or choose an entry in the list and click Properties. The Common Name List (Create|Edit) form opens.

3

If you are creating a common name list, configure the Displayed Name parameter.

4

Click on the Common Name List Entry tab and configure entries, as required.

1. Click Create, or choose an entry in the list and click Properties. The Common Name List Entry (Create|Edit) form opens.
2. Configure the required parameters.
3. Save your changes and close the Common Name List Entry (Create|Edit) form.

5

Click on the General tab and distribute the policy to NEs, as required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Close the open forms.

END OF STEPS

10.34 How do I configure an Enrollment over Secure Transport profile?

Note: This is applicable to 7250 IXR only.

10.34.1 Steps

1

Choose Administration→Security→NE PKI Authentication→Enrollment over Secure Transport from the NFM-P main menu. The Enrollment over Secure Transport form opens.

2

Click Create, or choose an entry in the list and click Properties. The Enrollment over Secure Transport (Create|Edit) form opens.

3

Configure the required parameters.

4

If you are creating an Enrollment over Secure Transport profile, configure the Profile parameter.

5

To specify a File Transmission Profile, click on the Select button.

6

Click Create, or choose an entry in the list and click Properties. The File Transmission Profile (Create|Edit) form opens.

See 10.36 “How do I create a file transmission profile?” (p. 322) for information about creating a File Transmission Profile to use with the Enrollment over Secure Transport profile.

7

To specify a TLS Client Profile, click on the Select button.

8

Click Create, or choose an entry in the list and click Properties. The TLS Client Profile (Create|Edit) form opens.

See Step 5 for information about creating a TLS Client profile to use with the Enrollment over Secure Transport profile.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Click Apply to save your changes.

10

Distribute the policy to NEs, as required.

11

Close the open forms.

END OF STEPS

10.35 How do I add an HSM to the NFM-P?

10.35.1 Purpose

Perform this procedure to add an 1830 SMS netHSM hardware security module to the NFM-P. In order to add an HSM:

- A user password in the form of a PKCS #11 PIN must be set.
- An HSM configuration file must be in the following directory on each NFM-P main server station: /opt/nsp/nfmp/server/nms/config/hsm/pkcs11
- HSM must be enabled in each main server configuration, as described in the *NSP Installation and Upgrade Guide* system installation procedures.

10.35.2 Steps

1

Choose Administration→Security→Hardware Security Module from the NFM-P main menu. The Hardware Security Module form opens.

2

Click Create→Hardware Security Module. The HSMConfig (Create) form opens.

3

Configure the parameters.

4

Click OK.

5

Test the connection to the HSM, if required.

1. In the Hardware Security Module list form, choose an HSM object and click Properties.
2. Click Test Connection to HSM.

   The test results are displayed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Save your changes and close the forms.

END OF STEPS

10.36 How do I create a file transmission profile?

10.36.1 Purpose

Follow this procedure to create a file transmission profile for use with a CRL URL entry when configuring a PKI certificate authority profile to use automatic CRL file download.

10.36.2 Steps

1

Choose Policies→ISA Policies→File Transmission Profile from the NFM-P main menu. The File Transmission Profile form opens.

2

Configure the required parameters.

3

Save your changes and close the form.

END OF STEPS

10.37 How do I perform CMPv2 actions?

10.37.1 Purpose

CMP is a protocol that runs between a Certification Authority, or CA, and an end entity to provide certificate management functions over HTTP.

10.37.2 Steps

1

Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the NFM-P main menu. The Select Site form opens.

2

Choose an NE in the list and click OK. The Site Security Public Key Infrastructure (Edit) form opens.

3

Click Admin Certificate and choose Perform CMPv2 Actions. The Admin Certificate form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Perform one of the following to configure the CA Profile Name parameter.

a. Select a CA profile.

b. Enter the profile name.

CMPv2 actions

5

Select a CMPv2 action from the drop-down menu beside the Type parameter in the Action panel. The following table lists the available CMPv2 actions. You can view the status of the last CMPv2 action performed on this site in the Last Action Status panel.

Table 10-1 CMPv2 actions

Action	See step
“Initial Registration” (p. 323)	Step 6
“Certificate Request” (p. 324)	Step 10
“Key Update” (p. 324)	Step 14
“Poll” (p. 324)	Step 18
“Clear Request” (p. 324)	Step 20
“Abort Request” (p. 325)	Step 22
“Manually Update CRL files” (p. 325)	Step 24

Initial Registration

6

Configure the required parameters in the Action panel.

7

Perform one of the following:

a. To perform an initial registration using a password, configure the required parameters in the Protection Algorithm - using Password panel.

b. To perform an initial registration using a certificate, configure the required parameters in the Protection Algorithm - using Certificate panel.

8

Click Apply to perform the action.

9

Go to Step 26 .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Certificate Request

10

Configure the required parameters in the Action panel.

11

Configure the required parameters in the Protection Algorithm - using Certificate panel.

12

Click Apply to perform the action.

13

Go to Step 26 .

Key Update

14

Configure the required parameters in the Action panel.

15

Configure the required parameters in the Protection Algorithm - using Certificate panel.

16

Click Apply to perform the action.

17

Go to Step 26 .

Poll

18

Click Apply to send the poll request.

19

Go to Step 26 .

Clear Request

20

Click Apply to send the clear request.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21

Go to Step 26 .

Abort Request

22

Click Apply to send the abort request.

23

Go to Step 26 .

Manually Update CRL files

24

Configure the Certificate Authority Profile parameter.

25

Click on the Execute button to send the update request.

26

Close the open forms.

END OF STEPS

10.38 How do I delete a security policy?

Note: When you delete site management access filter policies in which the Action parameter is set to deny, ensure that you modify the policy to set the parameter to permit before it is deleted, otherwise, the NFM-P may be isolated.

You cannot remove a site management access filter if the filter administrative state is up and the default action of the filter is set to deny or deny host unreachable.

If you attempt to delete an OmniSwitch RADIUS or TACACS+ security policy that is applied to an authentication service, the NFM-P generates a deployment error. You must use the OmniSwitch CLI to delete the policy from the authentication service before you can delete the policy from the NFM-P.

10.38.1 Steps

1

Choose the appropriate policy from one of the following.

a. The Administration→Security→*option* NFM-P main menu

b. The Policies→AAA Policies→*option* NFM-P main menu

The appropriate form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Set the filter criteria, if applicable.

3

Click Search. A policy list opens.

4

Choose a policy from the list.

5

Click Delete.

6

Click Yes. The policy is deleted.

END OF STEPS

10.39 How do I manually unlock a user account?

10.39.1 Steps

1

From the NFM-P main menu, choose Administration→Security→NE User Configuration. The NE User Configuration form opens.

2

Click Search. A list of user accounts appears.

3

Perform one of the following:

a. To unlock an NFM-P user, choose a user and click Unlock User. The user account is unlocked.

b. To unlock the local definition of a user on an NE, perform the following steps.

   Use this method to unlock a user account that is still within the lockout time period. The lockout time is set in 10.24 “How do I configure an NE password policy?” (p. 304).

   1. Choose a user account and click Properties. The NE User form opens.
   2. Click on the Local Definitions tab.
   3. Click Search. A list of NEs with local definitions for the user appears.
   4. Choose an NE and click Unlock User. The user account on the selected NE is unlocked.
   5. Close the NE User form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Close the NE User Configuration form.

END OF STEPS

10.40 How do I clear the password history of a user on a managed device?

10.40.1 Steps

1

Choose Administration→Security→NE User Configuration from the NFM-P main menu. The NE User Configuration form opens.

2

Configure the filters and click Search. A list of configured users appears.

3

Select a user and click Properties. The NE User (Edit) form opens.

4

Click on the Local Definitions tab. A list of sites with local definitions for the selected user appears.

5

Select one or more sites and click Clear Password History. A dialog box appears.

6

Click Yes to confirm the operation. The password history for the selected user at the specified sites is cleared.

7

Click OK. The NE User (Edit) form closes.

END OF STEPS

10.41 How do I clear collected statistics on a CPM filter?

10.41.1 Steps

1

From the NFM-P main menu, choose Administration→Security→NE CPM Filter. The CPM Filter form appears.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Click Search. A list of CPM filters appears.

3

Choose a CPM filter and click Properties. The CPM Filter (Edit) form appears.

4

Click on the Local Definitions tab.

5

Configure the filters and click Search. A list of CPM filter local definitions appears.

6

Choose a local definition and click Properties. The CPM Filter Local Policy form appears.

7

Click on the IPv4 Entries, IPv6 Entries, MAC Entries or Queues tab, depending on the type of statistic you need to clear.

8

Configure the filters and click Search. A list of filter entries appears.

9

Perform one of the following:

a. To clear specific entries, choose the entries you need to clear and click Clear Statistics on Entry.

b. To clear all entries, choose an entry and click Clear Statistics on All Entries. This button is not available in the Queues tab.

10

To view the status of all clear requests, perform the following:

1. Click on the Clear Statistics Status tab.
2. Configure the filters, and click Search. A list of clear requests appears.
3. Choose a clear request and click Properties. The status of the clear request appears.

11

Close the CPM Filter Local Policy, CPM Filter (Edit) and CPM Filter forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.42 How do I manage OCSP cache entries on an NE?

10.42.1 Steps

1

Choose Administration→Security→NE PKI Authentication→Site Public Key Infrastructure from the NFM-P main menu. The Select Site form opens.

2

Choose a managed device in the list and click OK. The Site Security Public Key Infrastructure (Edit) form opens.

3

Click on the OCSP Cache Entries tab.

4

Click Search. A list of OCSP cache entries for the site opens.

5

To clear cache entries, perform the following.

1. Click Admin Certificate and choose Clear OCSP Cache. The Admin Certificate Clear OCSP Cache form opens.
2. Enter the Entry ID number of the cache entry you need to clear in the Entry ID parameter. To clear all entries, leave the parameter blank.
3. Click Execute. The results of the clear operation appear in the results panel.
4. Click Close. The Admin Certificate Clear OCSP Cache form closes.

6

Click OK or Cancel. The Site Security Public Key Infrastructure (Edit) form closes.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.43 What is TCP enhanced authentication?

10.43.1 Overview



CAUTION

Service Disruption

It is recommended that you use only the NFM-P to create keys and key chains. Do not create a key or key chain directly on a managed NE using another interface, for example, a CLI. The NFM-P cannot obtain a TCP key secret value from an NE during resynchronization, so it cannot specify the key for use on another NE.

If a local NE key chain and the associated global NFM-P key chain differ after a resynchronization, the NFM-P raises an alarm.

This topic describes the NFM-P support of TCP enhanced authentication for NEs, based on the MD5 encryption mechanism described in RFC 2385, and the TCP Authentication Option (TCP-AO) as defined in RFC 5925 and 5926. NFM-P TCP enhanced authentication allows the use of powerful algorithms for authenticating routing messages.

The NFM-P uses a TCP extension to enhance BGP and LDP security by verifying administrative access at each end of a TCP connection. TCP peers update authentication keys during the lifetime of a connection.

An NFM-P operator with administrative privileges can create, delete, modify, and distribute TCP enhanced authentication components, and can perform an audit of a local key chain to compare it with the associated global key chain or other local key chains. The NFM-P TCP enhanced authentication components are called keys and key chains.

Global key chains are created in Draft mode. This allows operators to verify that the key chain is correctly configured before distribution to NEs. When the key chain is approved for distribution, you can change the global key chain to Released mode, which also distributes the key chain to existing local definitions. The NFM-P saves the latest released version of the global key chain.

10.43.2 TCP keys and key chains

A key is a data structure that is used to authenticate TCP segments. One or more keys can be associated with a TCP connection. Each key contains an identifier, a shared secret, an algorithm identifier, and information that specifies when the key is valid for authenticating the inbound and outbound segments.

A key chain is a list of up to 64 keys that is associated with a TCP connection. Each key within a key chain contains an identifier that is unique within the key chain. You can use the NFM-P to distribute a global key chain to multiple NEs and assign a key to multiple BGP or LDP instances.

The NFM-P treats global and local key chain management as it does policy management; depending on the distribution mode configuration of a local key chain, when you modify a global key chain using the NFM-P, all local instances can be updated to ensure that all instances of the key chain in the network are synchronized. See “Policies overview” in the *NSP NFM-P Classic Management User Guide* for information about global and local policy instances, policy distribution and distribution modes, and local policy audits.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

When the NFM-P attempts to synchronize the keys in a global key chain with the keys on an NE, the NE does not return the secret key value. After a key chain is deployed to an NE, the shared secret and the encryption algorithm cannot be modified. You can delete a key chain or key only when it is not in use by a protocol.

You can specify whether an NE uses a TCP key for sending packets, receiving packets, or both. Using keys that are configured for both, or send-receive, is general good practice because communication between NEs cannot be affected by assigning the wrong key type.

There are two classes of TCP keys:

- Active
- Eligible

Active keys

A key set contains one active key. An active key is a key that TCP uses to generate authentication information for outbound segments. You cannot delete the active key in a keychain.

Eligible keys

Each set of keys, called a key chain, contains zero or more eligible keys. An eligible key is a key that TCP uses to authenticate inbound segments.

10.44 Pathway: configure TCP enhanced authentication for NEs

10.44.1 Stages

1

Create a global key chain that contains at least one key; see 10.45 “How do I configure a global TCP key chain?” (p. 332) .

2

Distribute the key chain to the NEs; see 10.46 “How do I distribute global key chains to NEs?” (p. 333) .

3

Verify the distribution of a global key chain to the NEs; see 10.47 “How do I verify the distribution of a global key chain to NEs?” (p. 334) .

4

Assign the key chain to a routing protocol, such as BGP or LDP.

5

If required, identify the differences between a global and local policy or two local key chains; see 10.48 “How do I identify differences between a global and local key chain policy or two local key chains?” (p. 335) .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.45 How do I configure a global TCP key chain?

10.45.1 Steps

1

Choose Administration→Security→TCP KeyChains from the NFM-P main menu. The TCP KeyChains form opens.

2

Click Create or choose a key chain and click Properties. The KeyChain Create|Edit form opens.

3

Configure the required parameters.

4

Click on the KeyChain Key tab.

5

Click Create or choose a key chain key and click Properties. The KeyChain Key Create|Edit form opens.

6

CAUTION

Service Disruption

You must ensure bidirectional communication between NEs.

It is recommended that you choose the Send-receive option for the Key Direction parameter.

Configure the required parameters.

The End Time parameter is configurable only if the Key Direction parameter is set to Receive.

Note: You must set the Begin Time parameter to a time after the beginning of the current UNIX epoch. Do not set the parameter to 1970/01/01 00:00(TZ=UTC) or earlier.

Note: The NFM-P generates a random default value for the Key parameter. For greater security, it is recommended that you accept this value rather than manually enter a value. You cannot subsequently delete a TCP key chain or TCP key when the Admin State parameter for the key chain or key is set to In Service.

7

Save and close the forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10.46 How do I distribute global key chains to NEs?

10.46.1 Purpose

Perform the following procedure to distribute one or more global TCP key chains to one or more NEs. When you distribute a global key chain, a local key chain using the Sync With Global distribution mode allows the NE to receive the key chain.

CAUTION

Service Disruption

Releasing, distributing, or deleting a TCP keychain or TCP key can be service-affecting.

Ensure that you understand the implications of these operations before you proceed.

10.46.2 Steps

1

Choose Administration→Security→TCP KeyChains from the NFM-P main menu. The TCP KeyChains form opens.

2

Verify that none of the key chains in the list that you want to distribute are in Draft configuration mode and go to Step 4 . Otherwise go to Step 3 .

3

WARNING

Equipment Damage

Verify the local definitions before releasing a global key chain.

When you release a global key chain, the key chain is distributed to existing local definitions.

When a key chain is in Draft configuration mode, the Distribute button is disabled and the key chain cannot be distributed to an NE. You must first release the key chain for distribution.

To release a key chain:

1. Select the key chain entry and click Properties. The Key Chain (Edit) form opens.
2. Click Switch Mode to acknowledge the Configuration Mode change. The Release form opens.
3. Select the required NEs for release by moving the appropriate row entries from the Available Objects panel to the Selected Objects panel.

   See the policy management chapter in the *NSP NFM-P Classic Management User Guide* for more information on policy distribution.
4. Click on the Distribute button to release the key chain locally to devices.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5. Click Close. The Release form closes and the configuration mode of the key chain is changed to Released.
6. Close the Key Chain (Edit) form.

4

To distribute a key chain:

Note: Local definitions of key chains that use the Local Edit Only distribution mode do not allow their NEs to receive the distribution of a global key chain. You must set the distribution mode of a local key chain to Sync With Global if you need the associated NE to receive the distribution of a global key chain.

1. Select one or more key chains and click Distribute. The Distribute - KeyChain form opens.
2. Select the required NEs by moving the appropriate row entries from the Available Objects panel to the Selected Objects panel.
3. Click Distribute. The NFM-P distributes the key chains to the NEs.
4. Close the Distribute - KeyChain form. The TCP KeyChains form reappears.

5

To configure the distribution mode of a local definition:

1. Click Switch Distribution Mode. The Switch Distribution Mode form opens.
2. Choose Sync With Global, Local Edit Only, or All from the drop-down menu. Only the sites that are configured with the selected distribution mode are listed.
3. Choose one or more entries in the Available Local Policies panel and click on the right arrow. The chosen entries move to the Selected Local Policies panel.
4. Depending on the current distribution mode of the chosen entries, perform one of the following:
   - Click Sync With Global.
   - Click Local Edit Only.

   The distribution mode of the selected entries changes accordingly.
5. Close the Distribution Mode form.

6

Close the TCP KeyChains form.

END OF STEPS

10.47 How do I verify the distribution of a global key chain to NEs?

10.47.1 Steps

1

Choose Administration→Security→TCP KeyChains from the NFM-P main menu. The TCP KeyChains form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Select a key chain and click Properties. The KeyChain (Edit) form opens.

3

Click on the Local Definitions tab. The NEs that have a local instance of the key chain are displayed in a list.

4

View the list of NEs to confirm that the key chain is distributed to the required NEs.

5

Close the forms.

END OF STEPS

10.48 How do I identify differences between a global and local key chain policy or two local key chains?

10.48.1 Steps

1

Choose Administration→Security→TCP KeyChains from the NFM-P main menu. The TCP KeyChains form opens.

2

Choose Local from the Policy scope menu to select a local NE. The Select a Network Element form opens.

3

Select an NE and click OK. The NE IP address is displayed in the Local Node IP Address field.

4

Choose the local key chain that you need to compare with another key chain and click Properties. The KeyChain (Edit) form opens.

5

Click Local Audit On. The Local Audit form opens.

Note: You can cancel the local audit at any time by clicking Local Audit Off on the KeyChain (Edit) form.
The NFM-P does not identify differences between the Begin Time and End Time properties of key chains.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Perform one of the following from the Policy scope menu:

a. Choose Global and go to Step 7 .

b. Choose Local to choose an NE. The Select a Network Element form opens.

1. Select an NE and click OK. The NE IP address is displayed in the Local Node IP Address field.
2. Go to Step 7 .

7

Click OK. The Local Audit form closes and the appropriate global|local policy opens for comparison.

8

View the differences between the key chains by clicking on the tabs that are highlighted with an arrow icon to indicate that differences exist on the forms. An arrow icon beside a property indicates that the property is modified. In lists, new entries are highlighted in pink and modified entries are highlighted in purple.

9

Close the forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part III: NSP system administration

Overview

Purpose

This part of the *NSP System Administrator Guide* describes NSP system-level administration.

Contents

Chapter 11, NSP system configuration and management	339
Chapter 12, NSP cluster administration	363
Chapter 13, NSP cluster database administration	405
Chapter 14, NSP logging and monitoring	441

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11 NSP system configuration and management

11.1 What is NSP system configuration and management?

11.1.1 Description

The procedures in this chapter describe global system administration operations that may occasionally be required.

11.2 How do I change the nsp user password?

11.2.1 Purpose

Perform this procedure to change the password of the nsp user on a station in an NSP deployment.

11.2.2 Steps

1

Log in to the component station as the root user.

2

Open a console window.

3

Enter the following:

```
# passwd nsp ↵
```

The following prompt is displayed:

```
New Password:
```

4

Enter the new password and press ↵.

The following prompt is displayed:

```
Confirm New Password:
```

5

Enter the new password again and press ↵. The password is changed.

6

Record the new password and store it in a secure location.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Close the console window.

8

Log out of the component station.

END OF STEPS

11.3 How do I add an NSP feature package?

11.3.1 Steps

1

Contact Nokia to submit a new NSP license request for the system that includes the new feature package.

2

When you receive your updated license, install it in the NSP; see Step 5 in 1.4 “How do I install the NSP license?” (p. 25).

END OF STEPS

11.4 How do I update the NSP system configuration?

11.4.1 Purpose

Perform this procedure to update one or more aspects of the NSP deployment; for example:

- Change a parameter value.
- Add an installation option.
- Remove an installation option.

CAUTION

Service Disruption

Performing the procedure requires a restart of each NSP cluster, which is service-affecting. During the restart, the NSP may be temporarily unavailable.

You must perform the procedure only during a scheduled maintenance period.

Note: You must perform the procedure on each NSP cluster.

Note: In a DR deployment, you must perform the steps first on the standby NSP cluster.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.4.2 Steps

1

Open a terminal session.

2

Log in as the root or NSP admin user on the NSP deployer VM.

3

If you intend to remove any installation options, stop the NSP cluster; see 12.8 “How do I stop an NSP cluster?” (p. 371).

4

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

Add or remove installation options

5

Locate the **installationOptions** section in the **nsp** section, which resembles the following:

```
  installationOptions:
    - name: "NSP Platform - Base Services"
      id: platform-baseServices
    - name: "NSP Platform - Logging and Monitoring"
      id: platform-loggingMonitoring
#    - name: "Other Installation Option"
#      id: otherInstallationOption
```

6

To add an installation option, uncomment the installation option name and id lines by removing the leading # character from each line.

Note: You must preserve the leading spaces in each line.

7

To remove an installation option, convert the installation option name and id lines to comments by inserting a # character at the beginning of each line.

Note: You must preserve the spaces that follow the # character.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Update parameters

8

To enable a parameter that is currently disabled, uncomment the parameter line by removing the leading # character.

Note: You must preserve the leading spaces in the line.

9

To disable a parameter that is currently enabled, comment out the parameter line by restoring the leading # character.

Note: You must preserve the leading spaces in the line.

10

Configure parameter values, as required.

Save and deploy updated configuration

11

Save and close the nsp-config.yml file.

12

Enter the following to start the NSP cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member: nspdeployerctl --ask-pass install --config --deploy

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster starts, and the configuration update is put into effect.

13

Close the console window.

END OF STEPS

11.5 How do I regenerate an NSP system token?

11.5.1 Purpose

Perform this procedure to regenerate an NSP system token on either a standalone NSP deployment or a DR deployment.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.5.2 Steps

Standalone NSP

1

Log in as the root or NSP admin user on the NSP deployer VM.

2

Regenerate the system token:

```
# cd <NSP DEP build path>/bin
# ./nspdeployerctl secret -s system-token -n nsp-psa-restricted -r
system-token=32 update
```

END OF STEPS

11.5.3 DR NSP

1

Log in as the root or NSP admin user on the active and standby NSP deployer VMs.

2

Regenerate the system token on the active NSP deployer VM:

```
# cd <NSP DEP build path>/bin
# ./nspdeployerctl secret -s system-token -n nsp-psa-restricted -r
system-token=32 update
```

3

Fetch the regenerated system token from the active deployer VM:

```
# ./nspdeployerctl secret -s system-token -n nsp-psa-restricted -s
system-token -o /<Token_Save_Path>/regen-systoken.aes fetch
```

4

Copy the fetched token file (regen-systoken.aes) from the deployer VM to the standby deployer VM.

5

Install the regenerated system token secret on the standby deployer VM. On the standby deployer VM:

```
# cd <NSP DEP build path>/bin
# ./nspdeployerctl secret -n nsp-psa-restricted -s system-token -f
/<Token_Save_Path>/regen-systoken.aes update
```

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.6 PKI server access

11.6.1 Unblock or block PKI server access

Communications with the NSP PKI server is unblocked by default. However, you may need to unblock PKI server access before performing an administrative procedure on an NSP server. Use the commands below to unblock PKI server access at the beginning of an administrative process, and to block PKI server access at the end of your administrative process.

A PKI server access change may be required when configuring the following NSP servers:

- NFM-P main server
- NFM-P auxiliary server
- NFM-P main database
- NSP auxiliary database

If access to the PKI server is blocked during a procedure, unblock it by entering the following:

```
# /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/pki/pki-access
unblock ↵
```

After completing the procedure, block PKI server access by entering the following:

```
# /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/pki/pki-access
block ↵
```

11.7 How do I change the NSP cluster registry password?

11.7.1 Purpose

Perform this procedure to change the password of the NSP container registry administrator.

Note: The initial registry login attempt after the password change displays an error message that you can safely ignore.

11.7.2 Steps

1

Open a terminal session.

2

Log in as the root or NSP admin user on the NSP deployer VM.

3

Enter the following:

```
# cd /opt/nsp/nsp-registry-release-ID/bin ↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Enter the following:

```
# ./nspregistryctl update -p ↵
```

The following prompt is displayed.

```
Enter the current registry admin password:
```

5

Enter the current password.

The following prompt is displayed:

```
Enter the new registry admin password:
```

6

Create a new password; the password must:

- be a minimum of 10 characters
- include at least one:
  - uppercase character
  - lowercase character
  - digit
  - special character in the following list:
    ! # $ % & ( ) * + , - . / : ; = ? @ \ ^ _ { | }

7

Enter the new password.

The password is changed.

8

Record the new password and store it in a secure location.

9

Close the console window.

END OF STEPS

11.8 How do I remove the stale NSP allowlist entries?

11.8.1 Purpose

After an NSP system upgrade, hostname entries in the NSP allowlist that the NSP cannot resolve to an IP address may prevent NSP access. The following steps describe how to check for and remove stale NSP allowlist entries.

Note: You must perform the procedure in each data center of a DR NSP deployment.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.8.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-tomcat/ {print
$1;exit}') -it nspos-tomcat-0 -c nspos-tomcat -- bash ↵
```

4

Enter the following:

```
# grep "could not normalize or resolve host"
/opt/nsp/os/tomcat/logs/LaunchPad.log | grep -v grep ↵
```

Any stale allowlist entries are listed.

5

If the command returns any output lines like the following, the NSP allowlist includes hostname entries that you must remove; otherwise, go to Step 15.

```
<timestamp> could not normalize or resolve host: hostname
```

Record the hostname in each output line.

6

Enter the following to open a command shell on the PostgreSQL pod:

```
# kubectl exec -n  $(kubectl get pods -A | awk
'/nspos-postgresql-primary/ {print $1;exit}') --stdin --tty
nspos-postgresql-primary-0 -- /bin/bash ↵
```

7

Enter the following:

```
# cd /opt/nsp/os/pgsql/bin ↵
```

8

Enter the following to log in to the PostgreSQL database:

```
# ./psql -U username password ↵
```

where *username* and *password* are the PostgreSQL credentials, which are available from technical support

A PostgreSQL prompt is displayed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Enter the following:

select * from whitelist.whitelistedhost; ↵

The hosts in the NSP allowlist are listed; the hostname is in the rightmost column.

10

Record the dbid value of each hostname recorded in Step 5.

11

Enter the following to delete the unresolved hosts from the allowlist:

delete from whitelist.whitelistedhost where dbid in (*host1_ID*,*host2_ID*...*hostn_ID*); ↵

where *host1_ID* to *hostn_ID* is a comma-separated list of the IDs of the hosts to remove

The hosts are removed from the allowlist.

12

Enter the following to log out of the PostgreSQL database:

quit ↵

13

Close the console window.

END OF STEPS

11.9 How do I disable NSP websocket event notifications?

11.9.1 Purpose

Websocket-based events are used by some NSP functions. The following steps describe how to disable websocket event notifications, if required.

Note: The websocket connection used by the NSP may not function if a browser or any client is behind a proxy. Websocket communication through an entity between the websocket client and server, for example, a proxy server, firewall, or load balancer, is dependent on the entity configuration.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- # —root user
- bash$ —nsp user

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.9.2 Steps

1

Log in as the nsp user on the IP resource control server.

2

Open a console window.

3

Enter the following:

```
bash$ cd /opt/nsp/configure/config ↵
```

4

Open the wsc-security.conf file using a plain-text editor such as vi.

5

Modify the following section to read:

```
websocket {
enableEvents=false
}
```

6

Enter the following to restart the web server:

Note: If the NSP deployment is redundant, you must perform the step on each IP resource control server.

```
# systemctl restart nsp-tomcat ↵
```

The web server restarts, and websocket event notifications are disabled.

7

Close the console window.

END OF STEPS

11.10 How do I install custom Mistral actions for NSP Workflows?

11.10.1 Purpose

Perform this procedure to install custom Mistral actions created by Nokia Professional Services.

Before you start, the zip file containing the custom actions must be saved in a directory accessible to the root user. The zip file must follow Python directory packaging rules. The subdirectories in the zip file must be called `actions` and `expressions`.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

This procedure must be performed after an upgrade or DR switchover on the NSP deployer VM.

Note: The Mistral pods must be restarted for the custom actions to be applied in NSP Workflows. The restart will affect NSP Workflows operation.

If there are any files in **/opt/nsp/volumes/nsp-mistral-data**, they must be backed up to make them available for future use.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

11.10.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/wfm/bin ↵
```

4

Perform one of the following:

a. To copy the custom actions to the NSP without restarting the pods, enter the following:

```
# ./custom-actions.bash --install path ↵
```

b. To copy the custom actions to the NSP and restart the pods immediately, enter the following:

```
# ./custom-actions.bash --install path --restart ↵
```

where *path* is the absolute path of the zip file that contains the custom actions to install

5

To restart the Mistral pods, enter the following:

```
# ./custom-actions.bash --restart ↵
```

6

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.11 How do I remove Mistral actions from NSP?

11.11.1 Purpose

Perform this procedure to specify Mistral actions to drop, if required for network security. An action that is dropped cannot be called by a workflow. Dropping actions requires adding an environment variable to each Mistral engine in the NSP deployment.

You must perform the procedure on each NSP cluster in the deployment.

11.11.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Open each of the following files for editing:

- /opt/nsp/config/helm/values/wfm/nsp-mistral-engine/values.yaml
- /opt/nsp/config/helm/values/wfm/nsp-mistral-engine-triggers/values.yaml
- /opt/nsp/config/helm/values/lso/nsp-mistral-engine-lsom/values.yaml

4

Enter the following in the **env** section of each file:

`ACTIONS_DROP "`*`action_1 action_2 . . . action_n`*`"`

where *action_1* to `action_n` are the actions to drop

5

Obtain the engine name, namespace, chart name and chart version of each Mistral engine; enter the following:

`# helm list -A ↵`

Output like the following is displayed:

```
engine     namespace 1     timestamp  deployed chart_name-chart_
version     release
```

6

Obtain the Helm repository name and URL; enter the following:

`# helm repo list ↵`

Output like the following is displayed:

```
NAME            URL
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
nokia-nsp    repository URL
```

7

Enter the following for each Mistral engine:

```
# helm upgrade engine -n namespace chart_name --version chart_version
--repo repository URL -f path ↵
```

where

engine, *namespace*, *chart_name*, and *chart_version* are the values obtained in Step 5

repository and *URL* are the values obtained in Step 6

path is the path of the associated engine configuration file, and is one of:

- /opt/nsp/config/helm/values/wfm/nsp-mistral-engine/values.yaml
- /opt/nsp/config/helm/values/wfm/nsp-mistral-engine-triggers/values.yaml
- /opt/nsp/config/helm/values/lso/nsp-mistral-engine-lsom/values.yaml

The new environment variables are put in effect and the actions are unavailable to workflows.

8

Close the console window.

END OF STEPS

11.12 How do I configure a generic mediator?

11.12.1 Purpose

Use this procedure to install or uninstall a generic mediator to connect to an external controller. A generic mediator will handle authentication to the controller, allowing a call to be made to the controller from NSP without the need to provide credentials.

You can configure as many generic mediators as required, with different external controller parameters. The latest Helm chart and docker images are contained in the nsp configurator tar package with the name “nsp-mdt-generic-mediator”.

To provide generic mediator parameters to the NSP you must create a values.yaml file; see the Network Developer Portal for more information.

Naming

Each generic mediator must have a unique name.

Names must be unique in the following areas:

- the name of the instance in Helm
  You can allow Helm to autogenerate a unique name, however, using the -n option when installing the Helm chart will allow you to use a meaningful user identifiable name.
- the name of the pod and Kubernetes configuration

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

This is specified in the values.yaml file using the mediator_name value. When the name is given, the Kubernetes structures will be given a name like `nsp-mdt-<name>-mediator`. For example, to name the mediator SF1, enter the mediator_name: "SF1" in the values.yaml file. This will produce a pod and Kubernetes structures prefixed with nsp-mdt-SF1-mediator. If multiple words are in the name, they must be separated with a dash character (-).

The Helm instance name and the mediator_name do not have to be the same, however, using the same name may make alignment simpler.

Authentication information

Authentication information for the generic mediator is stored in a secret in the Kubernetes cluster. You need to create the secret before installing the generic mediator.

For information about the values to include in the secret, see the Network Developer Portal.

Certs files

Certs files may need to be copied into the pod for requests and authentication to work properly. This is done using a combination of the `copy_certs` and `certsFileName` properties, and the `--set-file` flag on the helm command.

When copy_certs is set to true, the NSP will attempt to copy a certs file into the pod in the `/opt/nsp/os/ssl/certs/custom` directory. Since the name of the certs file might be important and the mediator itself will not be aware of this, the file name to give this file is specified in the `certsFileName` value.

For example, if you have these values in the values.yaml file:

- `copy_certs: true`
- `certsFileName: "ca.pem"`

A file named ca.pem is created in the `/opt/nsp/os/ssl/certs/custom` directory.

If you specify `copy_certs: true` in the values.yaml file but do not add the `--set-file` flag to the helm command, the pod cannot initialize.

11.12.2 Steps

Perform Helm installation

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Create an NSP Kubernetes secret, see 7.13 “How do I add an NSP Kubernetes secret?” (p. 130).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Create a values.yaml file.

Ensure that the name of the secret created in Step 3 is configured in the `external_auth_secret_name` value.

5

Obtain the Helm repository name and URL; enter the following:

```
# helm repo list ↵
```

Output like the following is displayed:

```
NAME            URL
repository name     repository URL
```

6

Obtain the chart version for the nsp-mdt-generic-mediator chart; enter the following:

```
# helm search repo repository URL/repository
name/nsp-mdt-generic-mediator --versions↵
```

Output like the following is displayed:

```
NAME CHART VERSION APP VERSION DESCRIPTION
repository name/nsp-mdt-generic-mediator    chart_version
app_version Helm Chart for nsp-mdt-generic-mediator
```

7

Execute the Helm installation based on the following example:

```
# helm install mediator-instance-name repository URL/repository
name/nsp-mdt-generic-mediator --namespace namespace--version
chart_version -f values file --set-file externalControllerConfig.
externalControllerAuth.certsFile=certs file ↵
```

where

mediator instance name is the unique Helm instance name for the mediator, for example, generic-mediator-one

repository URL and *repository name* are the values obtained in Step 5

chart_version is the value obtained in Step 6

namespace is the Kubernetes namespace in use for existing mediators

values file is the path to the values.yaml file

certs file is the path to the certs file

If you do not want to copy certs files to the pod, the **`--set-file`** flag is not required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Perform Helm uninstallation

8

To uninstall a generic mediator, you must delete them using Helm. Execute the following:

```
# helm uninstall mediator-instance-name --namespace namespace ↵
```

where

mediator instance name is the mediator instance, for example, generic-mediator-one

namespace is the Kubernetes namespace

9

Close the console window.

END OF STEPS

11.13 How do I configure an NSP Workflows trigger framework?

11.13.1 Purpose

Use this procedure to install or uninstall a WFM framework. The WFM Trigger framework enables you to trigger workflows from an external system such as Git or HTTPS, without the need for NSP Workflows to monitor the external system directly.

The framework provided by NSP installs a single microservice that can handle at least one user -provided plugin installed into that microservice. The framework handles connections to the internal Kubernetes environment and to NSP Workflows, while the plug-in connects to the external system. The plugin must include a specified Python file to allow it to push to a Kafka topic in the NSP. From there, a Kafka Trigger can be created in NSP Workflows to trigger a workflow.

You can configure as many microservices as required, with different parameters. container images and Helm charts are provided in the Nokia Git repository.

This procedure provides general information. See the Network Developer Portal for more details.

Container image

You will need to use a container image generated from the base container image provided by NSP, that includes the code written to handle the external system. The name of the base image can be found either by browsing the NSP container repository or by looking at the provided defaulted values.yaml file.

Helm charts

A default values.yaml file is provided, and new values.yaml files must be derived from this one to get all the appropriate NSP-specific information that the pod needs to run. You need to change the following values:

- `pod_name`: Each pod must be given a unique pod name to avoid clashes over resources and so to install properly.
- `topic_name`: This specifies the topic name that messages will be sent on (and thus that the

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Kafka Trigger must listen on). The topic will always be wfm.trigger.<*topic_name*>. If this is not given, the `pod_name` will be used as the topic name.

- `pluginConfigFileName`: The file name of any config file that the user happens to be using. If this is not set, it defaults to `plugin.conf`.
- `pluginConfigFileInstallPath`: The install path of the config file. If this is not set, it defaults to `/opt/nsp/configure/config`.
- `pluginPythonClientFile`: The name and path of the client file that's importing the framework_server_client. If this is not set, it defaults to `/opt/nsp/launch_python_app.py`.
- `pluginCertsFileName`: The file name for any certs that are being used. If this is not set, it defaults to `plugincert.pem`.
- `pluginCertsInstallPath`: The install path for any certs that are being used. If this is not set, it defaults to `/opt/nsp`.

11.13.2 Steps

Perform Helm installation

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Execute the Helm installation based on the following example:

```
# helm install Helm_name Helm_path-f values_file --set-file
pluginCertsFile= certs_file --set-file pluginConfigFile=plugin_file ↵
```

where

Helm_name is the identifier of the Helm_chart

Helm_path is path to the Helm chart

values_file is the path to the values.yaml file

certs_file is the path to and filename of the certs file

plugin_file is the path to and filename of the plugin file

If you do not want to copy certs files to the pod, the **`--set-file pluginCertsFile`** flag is not required.

Perform Helm uninstallation

4

To uninstall a framework, you must delete them using Helm. Execute the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# helm uninstall Helm_name --namespace namespace -n $(kubectl get pods
-A | awk '/Helm_name/ {print$1;exit}') ↵
```

where

Helm_name is the framework Helm chart identifier

namespace is the Kubernetes namespace

5

Close the console window.

END OF STEPS

11.14 How do I manage NSP Analytics logging?

11.14.1 Purpose

The following steps describe how to enable Analytics logging, or to configure log levels of Analytics events for troubleshooting purposes.

By default, NSP Analytics logs only error events.

CAUTION

Excessive Resource Consumption Risk

Performing the procedure restarts NSP Analytics. Also, the logging may consume excessive disk space if logging is enabled for an extended period.

Perform the procedure only if required, and only for the period required to collect the log entries of interest. Contact technical support for assistance or more information.

11.14.2 Steps

1

Sign in to the NSP as an administrator.

2

Open Data Collection and Analysis Management, Analytics Server Management.

3

Click Logging Configuration on the navigation panel.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

CAUTION

Performance Degradation Risk

Enabling an NSP Analytics logging level other than the default, especially using the All option, or the auditing option in Step 5, may cause performance degradation as a result of excessive resource consumption.

Ensure that you enable a non-default logging option only as and when directed by technical support, and that the logging level is reset to the default afterward.

Use the **Server log level** drop-down list to set the log level, which is one of the following:

- Default—error logging only
- All—error, ad-hoc, and database transaction logging
- Ad Hoc—ad-hoc report logging
- SQL—database transaction logging only

5

Only as directed by technical support, use the **Auditing logs** drop-down to enable audit logging that includes all log levels, for example, information, warning, and error.

Note: It is strongly recommended that audit logging is not enabled for an extended period; contact technical support before you enable the option.

6

To enable or disable audit logging, use the **Auditing logs** drop-down.

7

Click **Update** to save the changes.

To cancel the changes, click **Refresh** (↻) or navigate to another view.

END OF STEPS

11.15 How do I resynchronize Analytics data dictionary objects?

11.15.1 Introduction

Analytic data dictionaries are used to synchronize dictionary objects from the PostgreSQL database to the auxiliary database to populate input controls in NSP Analytics reports. See the *NSP Analytics Report Catalog* for more information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.15.2 Steps

1

To resynchronize a specific data dictionary object, disable it, as described in the Network Developer Portal.

2

Re-enable the data dictionary object, as described in the Network Developer Portal.

Re-enabling causes a resynchronization of the dictionary object after an initial delay; the default is 12 minutes.

END OF STEPS

11.16 How do I verify disk performance for etcd?

11.16.1 Steps

1

Log in to the station as the root user.

2

Open a console window.

3

As the root user, enter the following:

```
# mkdir /var/lib/test ↵
# fio --rw=write --ioengine=sync --fdatasync=1 --directory=
/var/lib/test --size=22m --bs=3200 --name=mytest ↵
```

4

The command produces output like the following:

```
Starting 1 process
mytest: Laying out IO file (1 file / 22MiB)
Jobs: 1 (f=1)
mytest: (groupid=0, jobs=1): err= 0: pid=40944: Mon Jun 15 10:23:23
2020
  write: IOPS=7574, BW=16.6MiB/s (17.4MB/s)(21.0MiB/1324msec)
    clat (usec): min=4, max=261, avg= 9.50, stdev= 4.11
     lat (usec): min=4, max=262, avg= 9.67, stdev= 4.12
    clat percentiles (nsec):
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
     |  1.00th=[ 5536],  5.00th=[ 5728], 10.00th=[ 5920], 20.00th=[
6176],
     | 30.00th=[ 7584], 40.00th=[ 8896], 50.00th=[ 9408], 60.00th=[
9792],
     | 70.00th=[10432], 80.00th=[11584], 90.00th=[12864], 95.00th=
[14528],
     | 99.00th=[20352], 99.50th=[23168], 99.90th=[28800], 99.95th=
[42752],
     | 99.99th=[60672]
   bw (  KiB/s): min=16868, max=17258, per=100.00%, avg=17063.00,
stdev=275.77, samples=2
   iops        : min= 7510, max= 7684, avg=7597.00, stdev=123.04,
samples=2
  lat (usec)   : 10=64.21%, 20=34.68%, 50=1.08%, 100=0.02%, 500=0.01%
```

5

In the second block of output, which is shown below, the 99th percentile durations must be less than 10ms. In this block, each durations is less than 1ms.

```
fsync/fdatasync/sync_file_range:
    sync (usec): min=39, max=1174, avg=120.71, stdev=63.89
    sync percentiles (usec):
     |  1.00th=[   42],  5.00th=[   45], 10.00th=[   46], 20.00th=[
48],
     | 30.00th=[   52], 40.00th=[   71], 50.00th=[  153], 60.00th=[
159],
     | 70.00th=[  167], 80.00th=[  178], 90.00th=[  192], 95.00th=[
206],
     | 99.00th=[  229], 99.50th=[  239], 99.90th=[  355], 99.95th=[
416],
     | 99.99th=[  445]
  cpu          : usr=2.95%, sys=29.93%, ctx=15663, majf=0, minf=35
  IO depths    : 1=200.0%, 2=0.0%, 4=0.0%, 8=0.0%, 16=0.0%, 32=0.0%,
>=64=0.0%
     submit    : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
     complete  : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
     issued rwts: total=0,10029,0,0 short=10029,0,0,0 dropped=0,0,0,0
     latency   : target=0, window=0, percentile=100.00%, depth=1
```

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11.17 What are OpenSearch audit logs?

11.17.1 Description

When OpenSearch Audit Logging is enabled in NSP, the system begins capturing and recording security-relevant events generated within the OpenSearch cluster.

These audit logs provide detailed visibility into user actions, system access, and security-related operations, helping to ensure accountability, compliance, and traceability across the platform.

This feature captures REST API requests, Transport layer activities, and compliance activities, including

- Index creation, deletion, and update when logging is enabled for these operations
- Authentication success or failure
- Authorization failure
- Missing privileges
- SSL and certificate errors
- Other errors in audit.yml

OpenSearch audit logging is disabled by default.

11.17.2 Audit log indexes

Audit logs are created daily and have the index format security-audit-logs-*yyyy.MM.dd*

- Audit events are indexed in OpenSearch under security-audit-*.
- Indexing happens only when nsp.modules.logging.opensearchSecurityAuditLogs.enabled: true.
- Retention is controlled by retentionPeriodInDaysOverride
- Retention lifecycle is enforced by the ISM policy AuditLogCleanUpPolicy.
- In OpenSearch Dashboards, view audit logs in Discover using data view security-audit-*.

where *yyyy.MM.dd* is the year, month, and day

The logs are mapped to /usr/share/opensearch/plugins/opensearch-security/securityconfig/audit.yml.

The audit logs are retained according to the setting in the NSP configuration file.

11.18 How do I enable OpenSearch audit logging?

11.18.1 Steps

1

Open a terminal session.

2

Log in as the root or NSP admin user on the NSP deployer VM.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

Enable and configure OpenSearch audit logging

4

Enable audit logging as follows:

```
logging:
  opensearchSecurityAuditLogs:
    enabled: true
```

5

By default, READ and GET API requests are excluded from the audit logs.

Include these requests as follows:

```
logging:
  opensearchSecurityAuditLogs:
    includeReadOperations: true
```

6

The default retentionPeriodInDaysOverride for OpenSearch audit is zero (0).

Zero (0) means no explicit override, so the system uses the deployment profile default audit retention (typically five days for internal/lab profiles and 30 days for other profiles respectively).

You can override the retention period as follows:

```
logging:
  opensearchSecurityAuditLogs:
    retentionPeriodInDaysOverride: days
```

where *days* is retention period in days.

Example:

```
logging:
  opensearchSecurityAuditLogs:
    enabled: true
    includeReadOperations: true
    retentionPeriodInDaysOverride: 30
```

Save and deploy updated configuration

7

Save and close the nsp-config.yml file.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Enter the following to start the NSP cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member: nspdeployerctl --ask-pass install --config --deploy

```
# ./nspdeployerctl install --config --deploy ↵
```

The NSP cluster starts, and the configuration update is put into effect.

9

Close the console window.

END OF STEPS

11.19 How do I view OpenSearch audit logs?

11.19.1 Steps

1

As an NSP administrator, choose **System Health** from the NSP main menu.

2

In the System Health dashboard, login to the OpenSearch Dashboards.

3

Click Log Viewer.

4

View audit logs in the Discover panel.

Select the data view / index pattern security-audit-*

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12 NSP cluster administration

NSP cluster control and operation

12.1 How do I manage NSP clusters?

12.1.1 NSP cluster startup and shutdown

Low-level routine maintenance such as applying a RHEL OS patch to the hosts in an NSP Kubernetes cluster may require that you stop and start Kubernetes in the cluster.

Stopping Kubernetes in an NSP cluster stops the NSP software in the cluster, and creates a network management outage in a standalone deployment.

In a DR deployment, you can avoid a network management outage by stopping and starting the clusters in sequence, as specified in 12.7 “Pathway: stop and start DR NSP clusters” (p. 368).

12.1.2 Description

The following procedures describe the following basic Kubernetes administration operations for the NSP:

- starting and stopping clusters
- identifying the control-plane in a cluster
- displaying the DR status
- performing DR role switches
- recovering pods in CrashLoopBackOff state

12.1.3 NSP infrastructure health monitoring

The NSP has internal agents that monitor the NSP deployment infrastructure. An alarm in raised in response to the detection of one of the following NSP deployer VM fault conditions:

Note: An NSP deployer VM unreachability alarm clears automatically when reachability is restored.

- NSP deployer VM unreachability
- Harbor registry unavailability
- excessive disk consumption

12.2 How do I view the status of all Kubernetes pods?

12.2.1 Purpose

Perform this procedure to view the status of all Kubernetes pods in an NSP cluster.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.2.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↲
```

2

Open a console window.

3

Enter the following command to view a list of pods in the NSP cluster:

```
# kubectl get pods -A ↲
```

The Kubernetes pods are listed.

END OF STEPS

12.3 How do I retrieve pod information?

12.3.1 Steps

1

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↲
```

2

Open a console window.

3

Enter the following to view information about a specific pod:

```
# kubectl describe pod --namespace pod_namespace pod_name ↲
```

where *pod_namespace* is the name of the pod's namespace and *pod_name* is the name of the pod

The command output includes many parameters, including any events associated with the pod. For example:

```
Type     Reason            Age         From               Message
----     ------            ----        ----               -------
Warning  FailedScheduling  <unknown>   default-scheduler  0/1 nodes are
available: 1 Insufficient memory.
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: Ensure the full name of the pod is entered for *pod_name*. To find the full name of a pod, see the procedure 12.2 “How do I view the status of all Kubernetes pods?” (p. 363).

END OF STEPS

12.4 How do I retrieve a list of cluster members?

12.4.1 Steps

1

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↵
```

2

Enter the following periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until the output lists only the following:

- pods in kube-system namespace
- nsp-backup-storage pod

```
# kubectl get pods -A ↵
```

The pods are listed.

3

Open a console window.

4

Enter the following to list the NSP cluster members:

```
# kubectl get nodes ↵
```

END OF STEPS

12.5 How do I retrieve cluster member information?

12.5.1 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Enter the following to view information about a specific member:

kubectl describe nodes *node_name* ↵

where *node_name* is the name of the member to view

4

The command output includes member information such as the following:

- member status; for example:

```
Type Status LastHeartbeatTime LastTransitionTime Reason Message
---- ------ ----------------- ------------------ ------ -------
NetworkUnavailable False Wed, 30 Sep 2020 12:19:23 -0400 Wed, 30 Sep 2020 12:19:23 -0400
CalicoIsUp Calico is running on this node
```

- member resource capacity; for example:

```
Capacity:
  cpu:                24
  ephemeral-storage:  67092472Ki
  hugepages-1Gi:      0
  hugepages-2Mi:      0
  memory:             64381888Ki
  pods:               110
```

- running pods on the member; for example:

```
Namespace Name CPU Requests CPU Limits Memory Requests Memory Limits AGE
--------- ---- ------------ ---------- --------------- ------------- ---
default nginx-ingress-controller-8fj7s 100m (0%) 12 (37%) 500Mi (0%) 1000Mi (0%) 7h9m
default nspos-app1-tomcat-8597d67787-wdgxd 5100m (16%) 12100m (38%) 17230Mi (13%) 17230Mi
(13%) 7h10m
default nspos-neo4j-core-default-1 2050m (6%) 2050m (6%) 2650Mi (2%) 2650Mi (2%) 7h10m
default nspos-postgresql-primary-0 6050m (19%) 6050m (19%) 1290Mi (1%) 1290Mi (1%) 7h9m
```

- resources allocated to the member; for example:

```
Resource           Requests          Limits
--------           --------          ------
cpu                22870m (71%)      41150m (129%)
memory             42120228Ki (32%)  44290630912 (33%)
ephemeral-storage  0 (0%)            0 (0%)
```

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.6 How do I change internal user account names and passwords?

12.6.1 Purpose

For enhanced security, NSP allows reconfiguration of internal account user names and passwords. NSP uses a number of internal accounts for its applications. User names and passwords for these accounts are held in Kubernetes secrets and cannot be managed through the NSP GUI.

When an NSP system is installed and the Kubernetes secrets are created, those secrets receive randomized user names and passwords, or specific values as defined by the administrator. After installation, you can regenerate or reconfigure the secrets as needed.

When an NSP system is upgraded from an earlier release, the existing Kubernetes secrets are retained. When the secret install runs during the upgrade process, only missing secrets are generated. You may choose to update any secrets at upgrade time or after the upgrade, as desired. The internal account user names and password can be changed by updating the Kubernetes secret associated with that internal account.

NSP uses the following Kubernetes secrets that contain internal user name and password information:

- opensearch-user-secret
- keycloak-masterrealm-secret
- keycloak-altiplanoadmin-secret
- csf-rabbitmq-secret
- csf-rabbitmq-secret-restricted
- grafana



WARNING

Internal communication disruption

Changing an internal account kubernetes secret could disrupt communications within an NSP deployment.

12.6.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

The following command modifies an internal account secret. You can select a kubernetes secret from the list above.

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
# ./nspdeployerctl secret -n nsp-psa-restricted -s <secret> -v
<username attribute>=<new username> -p  <password attribute>=<new
password> update ↵
```

where

<secret> is the name of the kubernetes secret being modified

<username attribute> is user name attribute in the secret

<new username> is the new user name for the secret

<password attribute> is the password attribute in the secret

<new password> is the new password for the secret

END OF STEPS

12.7 Pathway: stop and start DR NSP clusters

12.7.1 Description

CAUTION

System Degradation

If the primary NSP cluster and associated primary components outside the cluster are not in the same data center, the maintenance shutdown described in this pathway may cause an undesired DR switchover of one or more components, which can be service-affecting.

Before you attempt to use this pathway, you must ensure that the primary NSP cluster and associated primary components outside the cluster are in the same data center. If not, perform the appropriate procedure to ensure that all component roles in each data center are aligned.

The following is the sequence of high-level actions required to stop and start the primary and standby NSP clusters in a graceful manner for maintenance purposes.

See the following procedures for information about stopping and starting a cluster:

- 12.8 “How do I stop an NSP cluster?” (p. 371)
- 12.9 “How do I start an NSP cluster?” (p. 373)

12.7.2 Stages

Perform orderly shutdown of standby components outside NSP cluster

1

If the NSP deployment includes an auxiliary database, stop the auxiliary database cluster in the standby data center, as described in 20.4 “How do I stop an auxiliary database cluster?” (p. 525).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

If the NSP deployment includes the NFM-P, perform the following steps.

1. Stop each Reserved NFM-P auxiliary server of the standby main server; see 21.7 “How do I stop an auxiliary server?” (p. 597).
2. Stop each Preferred NFM-P auxiliary server of the standby main server; see 21.7 “How do I stop an auxiliary server?” (p. 597).
3. Stop the standby main server; see 21.3 “How do I stop a main server?” (p. 593).
4. Stop the standby main database; see 21.5 “How do I stop a main database?” (p. 595).

Perform standby NSP cluster maintenance

3

Stop the standby NSP cluster, as described in 12.8 “How do I stop an NSP cluster?” (p. 371).

4

Perform the required maintenance on the standby cluster.

5

Start the standby cluster, as described in 12.9 “How do I start an NSP cluster?” (p. 373).

Switch NSP cluster roles

6

Perform a switchover to change the standby cluster role to primary, as described in 15.4 “How do I perform an NSP DR switchover from the NSP UI?” (p. 453).

The standby cluster assumes the primary role.

Perform orderly startup of standby components outside cluster

7

If the NSP deployment includes the NFM-P, perform the following steps.

1. Start the former standby main database; see 21.4 “How do I start a main database?” (p. 594).
2. Start the former standby main server; see 21.2 “How do I start a main server?” (p. 593).
3. Start each Preferred NFM-P auxiliary server of the former standby main server; see 21.6 “How do I start an auxiliary server?” (p. 596).
4. Start each Reserved NFM-P auxiliary server of the former standby main server; see 21.6 “How do I start an auxiliary server?” (p. 596).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

If the NSP deployment includes an auxiliary database, start the auxiliary database cluster in the former standby data center; see 20.3 “How do I start an auxiliary database cluster?” (p. 523).

Perform orderly shutdown of former primary components outside NSP cluster

9

If the NSP deployment includes the NFM-P, perform the following steps.

1. Stop each Preferred NFM-P auxiliary server of the former primary main server; see 21.7 “How do I stop an auxiliary server?” (p. 597).
2. Stop each Reserved NFM-P auxiliary server of the former primary main server; see 21.7 “How do I stop an auxiliary server?” (p. 597).
3. Stop the former primary main server; see 21.3 “How do I stop a main server?” (p. 593).
4. Stop the former primary main database; see 21.5 “How do I stop a main database?” (p. 595).

Perform former primary NSP cluster maintenance

10

Stop the former primary cluster, as described in 12.8 “How do I stop an NSP cluster?” (p. 371).

11

Perform the required maintenance on the former primary cluster.

12

Start the former primary cluster, as described in 12.9 “How do I start an NSP cluster?” (p. 373).

Perform orderly startup of former primary components outside cluster

13

If the NSP deployment includes the NFM-P, perform the following steps.

1. Start the former primary main database; see 21.4 “How do I start a main database?” (p. 594).
2. Start the former primary main server; see 21.2 “How do I start a main server?” (p. 593).
3. Start each Preferred NFM-P auxiliary server of the former primary main server; see 21.6 “How do I start an auxiliary server?” (p. 596).
4. Start each Reserved NFM-P auxiliary server of the former primary main server; see 21.6 “How do I start an auxiliary server?” (p. 596).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14

If the NSP deployment includes an auxiliary database, start the auxiliary database cluster in the former primary data center; see 20.3 “How do I start an auxiliary database cluster?” (p. 523).

Restore initial primary/standby NSP cluster roles

15

If required, perform a switchover to restore the initial primary and standby roles, as described in 15.4 “How do I perform an NSP DR switchover from the NSP UI?” (p. 453).

12.8 How do I stop an NSP cluster?

12.8.1 Purpose

CAUTION

Network Management Disruption or Outage

Performing the procedure in a standalone deployment completely stops the NSP and creates a network management outage that persists until you start the cluster. In a DR deployment, stopping an NSP cluster may initiate a server switchover that may temporarily affect network management.

Perform the procedure only during a scheduled maintenance period and under the guidance of technical support.

The following steps describe how to stop the Kubernetes software in an NSP cluster, for example, when the NSP hosts in the cluster require maintenance, or for cluster decommissioning.

Note: If you are stopping the NSP clusters in a DR deployment, ensure that you perform the procedure at the appropriate stage of 12.7 “Pathway: stop and start DR NSP clusters” (p. 368).

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

Note: If the cluster is SELinux-enabled, it must be placed in SELinux permissive mode prior to stopping; see 12.10 “How do I switch an NSP cluster between SELinux modes?” (p. 374).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.8.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

4

Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

```
deleteOnUndeploy:false
```

5

Save and close the file.

6

Enter the following:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass uninstall --undeploy

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl uninstall
--undeploy ↲
```

The NSP cluster stops.

7

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↲
```

8

Open a console window.

9

Enter the following periodically to display the Kubernetes cluster status:

```
# kubectl get pods -A ↲
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The NSP cluster is stopped when only the following namespaces and associated pods appear in the output, for example:

```
NAMESPACE           NAME                   READY   STATUS    RESTARTS
AGE
kube-system         calico-node-99d28      1/1     Running   0
age
...
kube-system         kube-apiserver-node1   1/1     Running   7
age
kube-system         kube-proxy-c9vch       1/1     Running   0
age
metallb-system      speaker-fsw6b          1/1     Running   0
age
metallb-system      speaker-nhslk          1/1     Running   0
age
nsp-psa-restricted  nsp-backup-storage-0   1/1     Running   0
age
```

The number of pods running in the kube-system and metallb-system namespaces can vary. There is also one nsp-backup-storage pod. These pods are expected to remain running after NSP is uninstalled.

10

When the NSP cluster is stopped, close the console window.

END OF STEPS

12.9 How do I start an NSP cluster?

12.9.1 Purpose

The following steps describe how to start the Kubernetes software in an NSP cluster.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

Note: If the cluster is SELinux-enabled, it must be placed in SELinux permissive mode prior to startup; see 12.10 “How do I switch an NSP cluster between SELinux modes?” (p. 374).

12.9.2 Steps

1

Open a terminal session to the NSP deployer VM.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Log in as the root or NSP admin user.

3

Enter the following:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --deploy

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --deploy ↵
```

The NSP cluster starts.

4

Log in as the root or NSP admin user on the NSP deployter host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↵
```

5

Open a console window.

6

Enter the following periodically to display the Kubernetes cluster status:

```
# kubectl get pods -A ↵
```

The NSP is operational when the status of each pod is Running or Completed.

7

When the NSP cluster is operational, close the console window.

END OF STEPS

12.10 How do I switch an NSP cluster between SELinux modes?

12.10.1 Purpose

Perform this procedure to change an SELinux-enabled NSP cluster between permissive and enforcing mode.

12.10.2 Steps

1

Log in as the root user on the NSP cluster node.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/nsp-deployer/tools/selinux/tools/bin ↵
```

4

Do one of the following:

- Enter the following to switch to permissive mode:

  ```
  # ./selinuxenable.sh -p ↵
  ```

  The SELinux mode is set to permissive.
- Enter the following to switch to enforcing mode:

  ```
  # ./selinuxenable.sh -e ↵
  ```

  The SELinux mode is set to enforcing.

END OF STEPS

12.11 How do I identify the control-planes in an NSP cluster?

12.11.1 Purpose

The following steps describe how to list the NSP cluster VMs and identify which have the control-plane role.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

12.11.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Enter the following:

```
# kubectl get nodes -o wide ↵
```

A list of VMs like the following is displayed.

```
NAME    STATUS   ROLES    AGE   VERSION   INTERNAL-IP
EXTERNAL-IP
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
node1   Ready    control-plane   nd   version   int_IP   ext_IP
node2   Ready    <none>   nd   version   int_IP   ext_IP
node3   Ready    <none>   nd   version   int_IP   ext_IP
```

4

View the ROLES entries to identify the nodes with the control-plane role.

5

Close the console window.

END OF STEPS

12.12 How do I display the NSP cluster status?

12.12.1 Purpose

The following steps describe how to view the status of standalone or redundant NSP clusters.

Note: You require root user privileges on each NSP cluster VM in each data center.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

12.12.2 Steps

1

Log in as the root or NSP admin user on any NSP cluster VM.

2

Open a console window.

3

In a standalone deployment, enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nsp-role-manager/
{print $1;exit}') -it $(kubectl get pods -A | awk '/nsp-role-manager/
{print $2;exit}') -c role-manager -- /opt/nsp/os/rolemgr/bin/rmgrctl
status ↵
```

Cluster status output like the following is displayed:

```
Site:   cluster_name
Status: active
Since:  timestamp
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

In a DR deployment, enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nsp-role-manager/
{print $1;exit}') -it $(kubectl get pods -A | awk '/nsp-role-manager/
{print $2;exit}') -c role-manager -- /opt/nsp/os/rolemgr/bin/rmgrctl
statusAll ↵
```

Cluster status output like the following is displayed:

```
Site:   primary_cluster_name
Status: active
Since:  timestamp
Site:   standby_cluster_name
Status: standby
Since:  timestamp
```

5

Close the console window.

END OF STEPS

12.13 How do I restart a Kubernetes pod?

12.13.1 Purpose

Perform this procedure to restart a Kubernetes pod in an NSP cluster; for example, as directed by technical support during a maintenance operation.

12.13.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Enter the following to list the pod that you need to restart:

```
# kubectl get pods -A | grep string ↵
```

where *string* is part of the pod name

The pod instance names that include *string* are listed.

4

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

kubectl delete pod *pod_name* -n $(kubectl get pods -A | awk '/*pod_name*/ {print $1;exit}') ↵

where *pod_name* is the name of the pod to restart

The pod is deleted and recreated.

5

Close the console window.

END OF STEPS

12.14 How do I delete Errored or Evicted pods?

12.14.1 Purpose

In situations such as the following, one or more NSP pods may enter the Errored or Evicted state. The NSP raises an alarm against each such pod, and a CLI query displays them, as shown below:

```
namespace     pod_a     1/1     Running   0    18m
namespace     pod_b     1/1     Errored   0    18m
namespace     pod_c     0/1     Evicted   0    19m
```

An Errored pod is typically the result of an unplanned VM reboot.

A pod is typically Evicted because of insufficient storage space on the host node, which is often called disk pressure.

In either case, the Kubernetes orchestrater reschedules the pod to a different node in the NSP cluster.

Each Errored or Evicted pod is preserved for forensic analysis, but consumes no host resources. When the investigation of the pod failure is complete, you can safely delete the preserved pod.

Perform the following procedure to delete all Errored or Evicted pods in an NSP cluster.

12.14.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_kubeconfig ↵

2

Open a console window.

3

Enter the following to list the pods in the NSP cluster.

kubectl get pods -A ↵

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The pods are listed.

4

Enter the following:

```
# kubectl get pods -A | awk '$4 ~ /Evicted|Error/{print $1, $2}' |
xargs -n 2 kubectl delete pod -n ↵
```

Each Errored or Evicted pod is deleted.

5

Enter the following:

```
# kubectl get pods -A ↵
```

The pods are listed.

6

Verify that no Errored or Evicted pods remain in the cluster.

7

Close the console window.

END OF STEPS

12.15 How do I recover pods in CrashLoopBackOff state?

12.15.1 Purpose

When a container in a pod fails repeatedly, Kubernetes sets the pod to CrashLoopBackOff and increases the delay between restart attempts. An NSP pod in this state is listed with a STATUS of CrashLoopBackOff, as shown below:

```
namespace pod_name 0/1 CrashLoopBackOff 5 12m
```

Use this procedure to inspect container logs and recover when logs report *exec format error*, which indicates that the container image on the node hosting the pod is corrupted. Scaling the workload to zero replicas and removing the corrupted image from the node allows Kubernetes to pull a fresh image when the workload is scaled back up.

Other log messages may indicate configuration errors, missing secrets, or registry image-pull failures. For those cases, collect the logs and contact Nokia support before taking corrective action beyond log collection. If a registry or TLS certificate problem is suspected, see 7.6 “How do I update the Kubernetes registry TLS certificate?” (p. 117).

Note: To list all pods or view pod events, see 12.2 “How do I view the status of all Kubernetes pods?” (p. 363) and 12.3 “How do I retrieve pod information?” (p. 364).

12.15.2 Steps

1

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↲
```

2

Open a console window.

3

Enter the following to list the pods in the NSP cluster:

```
# kubectl get pods -A ↲
```

Identify the pod that has a STATUS value of CrashLoopBackOff and record its namespace and name.

4

Enter the following to identify the cluster node that hosts the pod:

```
# kubectl get pod pod_name -n namespace -o wide ↲
```

where *pod_name* is the name of the pod in CrashLoopBackOff state and *namespace* is the pod namespace

Record the NODE value; you require this node when you remove the corrupted container image.

5

Enter the following to view the container logs for the pod:

```
# kubectl logs pod_name -n namespace ↲
```

If the pod has multiple containers, Kubernetes may default to a sidecar container and display a message such as the following:

```
Defaulted container "container_a" out of: container_a, container_b,
container_c (init)
```

Enter the following to view logs for the failing container:

```
# kubectl logs pod_name -n namespace -c container_name ↲
```

where *container_name* is the name of the container that is crashing

Review the log output to determine the cause of the failure. For example, the following output indicates a corrupted container image on the node:

```
exec /binary: exec format error
```

Note: If the log output does not contain *exec format error*, contact technical support with the log output before you continue.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

If the log output contains *exec format error*, scale the workload that manages the pod to zero replicas.

On the NSP deployer host, do one of the following:

- If the pod is managed by a StatefulSet, enter the following:

  # **kubectl scale statefulset *workload_name* -n *namespace* --replicas=0** ↵

  where *workload_name* is the name of the StatefulSet
- If the pod is managed by a Deployment, enter the following:

  # **kubectl scale deployment *workload_name* -n *namespace* --replicas=0** ↵

  where *workload_name* is the name of the Deployment

The workload stops and the pod is terminated.

7

Log in as the root user on the NSP cluster node recorded in the NODE column.

8

Open a console window on the cluster node.

9

Enter the following to list the container images on the node:

crictl images ↵

Identify the image ID of the image used by the pod that was in CrashLoopBackOff state.

10

Enter the following to remove the corrupted image:

crictl rmi *image_id* ↵

where *image_id* is the image ID from the previous step.

To retrieve the container image ID, run # **kubectl describe pod *pod-name* -n *namespace***

11

Enter the following to remove unused images:

crictl rmi --prune ↵

Unused images are removed from the node.

12

Close the console window on the cluster node.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↵
```

14

Open a console window.

15

Scale the workload back to one replica.

Do one of the following:

- If the pod is managed by a StatefulSet, enter the following:

  ```
  # kubectl scale statefulset workload_name -n namespace --replicas=1
  ↵
  ```

- If the pod is managed by a Deployment, enter the following:

  ```
  # kubectl scale deployment workload_name -n namespace --replicas=1 ↵
  ```

Kubernetes recreates the pod and pulls a fresh container image from the registry.

16

Enter the following periodically until the pod STATUS value is Running:

```
# kubectl get pods -A ↵
```

The pods are listed.

17

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NSP cluster lifecycle management

12.16 What is Kubernetes cluster lifecycle management?

12.16.1 Description

The following procedures describe NSP Kubernetes cluster lifecycle management operations that may occasionally be required, such as:

- moving a pod to a different cluster node
- adding, removing, and replacing cluster nodes
- backing up and restoring the NSP deployer VM configuration

12.17 How do I move a Kubernetes pod to a different node?

12.17.1 Purpose

The following steps describe how to move a non-pinned Kubernetes pod to a different node in an NSP cluster. This action may be required, for example, when you need to allocate additional node capacity to a pod that is pinned to a specific node.

12.17.2 Steps

CAUTION

System Degradation

The procedure includes operations that fundamentally reconfigure the NSP system.

You must contact Nokia support for guidance before you attempt to perform the procedure.

1

Log in as the root or NSP admin user on the NSP deployer host and enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↵
```

2

Open a console window.

3

Enter the following:

```
# kubectl get pods -A -o wide ↵
```

The pods are listed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Enter the following to list all nodes:

kubectl get nodes ↵

5

Enter the following:

kubectl describe nodes *node* ↵

where *node* is the name of the node that has the pod to move

The node resources are listed.

6

Record the Memory Requests and CPU Requests values.

7

List the nodes to ensure that another node has sufficient capacity for the pod to move:

kubectl describe nodes ↵

The nodes are listed.

8

View the Allocated resources value for each node to ensure that sufficient capacity exists according to the Requests value.

9

Enter the following to cordon the node that the pod is currently running on in order to prevent new pods from being scheduled on the node:

kubectl cordon *node* ↵

where *node* is the name of the node to cordon

Note: Existing pods on the node continue to run and are unaffected.

10

Restart the pod you intend to move.

1. Enter the following:

   # **kubectl get deployments -A** ↵

   The pods are listed.

2. Enter the following to stop the pod:

   # **kubectl scale deployment *pod* -n $(kubectl get pods -A | awk '/*pod*/ {print$1;exit}') --replicas=0** ↵

   where *pod* is the pod name

3. Enter the following to start the pod:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# kubectl scale deployment pod -n $(kubectl get pods -A | awk
'/pod/ {print$1;exit}') --replicas=1 ↵
```

The pod is scheduled on a different node.

11

Verify that the pod is successfully moved to another node; enter the following:

```
# kubectl get pods -A -o wide ↵
```

The pods are listed.

12

Uncordon the node; enter the following:

```
# kubectl uncordon node ↵
```

where *node* is the node name

The node enters the Initializing state, and then moves to the "Running" state.

13

If the pod remains in the Pending state, no other node may have sufficient resources to host the pod; enter the following:

```
# kubectl describe pod pod_name  -n $(kubectl get pods -A | awk
'/<pod_name>/ {print$1;exit}') ↵
```

Information about why the pod remains in the Pending state is displayed:

14

Close the console window.

END OF STEPS

12.18 How do I add an NSP cluster node?

12.18.1 Purpose

Perform this procedure to create a new worker node in an NSP cluster. The new node can run pods that do not require the local-provisioner (RWO), such as pods that are not pinned to a specific node.

Note: The procedure does not describe the addition of control-plane nodes. To add control-plane nodes to a cluster, see “To enlarge an NSP deployment” in the *NSP Installation and Upgrade Guide*.

Note: If root access for remote operations is disabled in the NSP configuration, remote operations such as SSH and SCP as the root user are not permitted within an NSP cluster. Steps that describe such an operation as the root user must be performed as the designated non-root user with sudoer privileges.

For simplicity, such steps describe only root-user access.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.18.2 Steps



CAUTION

System Degradation

The procedure includes operations that fundamentally reconfigure the NSP system.

You must contact Nokia support for guidance before you attempt to perform the procedure.

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Open the following file using a plain-text editor such as vi:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

4

Add the new node to the **hosts** section, as shown below; see the descriptive text at the head of the file for parameter information.

```
nodeName: node5
nodeIp: 192.168.98.196
accessIp: 203.0.113.5
```

5

Save and close the file.

6

Create a backup copy of the updated k8s-deployer.yml file, and transfer the backup copy to a station that is separate from the NSP system and preferably in a remote facility.

Note: The backup file is crucial in the event of an NSP deployer VM failure, so must be available from a separate station.

7

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

8

Enter the following to create the cluster configuration:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

./nspk8sctl config -c ↵

The following is displayed when the creation is complete:

✓ Cluster hosts configuration is created at: /opt/nsp/nsp-k8s-deployer-*release-ID*/config/hosts.yml

9

You must generate an SSH key for password-free NSP deployer VM access to the new NSP cluster VM.

Enter the following:

ssh-keygen -N "" -f *path* -t rsa ↵

where *path* is the SSH key file path, for example, /home/*user*/.ssh/id_rsa

An SSH key is generated.

10

Enter the following for each NSP cluster VM to distribute the key to the VM.

ssh-copy-id -i *key_file user*@*address* ↵

where

user is the designated NSP ansible user, if root-user access is restricted; otherwise, *user*@ is not required

key_file is the SSH key file, for example, /home/*user*/.ssh/id_rsa.pub

address is the IP address of the new VM

11

Close the VM console window.

12

Enter the following on the NSP deployer VM:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspk8sctl --ask-pass install

./nspk8sctl install ↵

The updated NSP cluster is deployed.

13

Log in as the root or NSP admin user on the NSP cluster host.

14

Enter the following to verify that the new node is added to the cluster:

kubectl get nodes ↵

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

An action such as the following causes pod deployment on the new node:

- moving a pod to the node, as described in 12.17 “How do I move a Kubernetes pod to a different node?” (p. 383)
- enabling additional NSP features that do not require the local-provisioner (RWO), as described in the NSP Installation and Upgrade Guide

15

Back up the NSP cluster data, as described in 13.4 “How do I back up the NSP cluster databases?” (p. 410)

16

Close the open console windows.

END OF STEPS

12.19 How do I remove an NSP cluster node?

12.19.1 Purpose

The following steps describe how to remove a node from an NSP cluster.

Note: You can use the procedure to remove only a node added using procedure 12.18 “How do I add an NSP cluster node?” (p. 385).

12.19.2 Steps

CAUTION

System Degradation

The procedure includes operations that fundamentally reconfigure the NSP system.

You must contact Nokia support for guidance before you attempt to perform the procedure.

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Enter the following:

```
# kubectl get nodes ↵
```

The NSP cluster nodes are listed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Record the name of the node that you intend to remove.

5

Enter the following to stop all pods that are running on the node:

kubectl drain *node* --ignore-daemonsets --delete-emptydir-data ↵

where *node* is the name of the node that you intend to remove

6

Enter the following:

kubectl delete node *name* ↵

where *name* is the name of the node to remove

The node is removed from the cluster.

7

Enter the following:

kubectl get nodes ↵

The NSP cluster nodes are listed.

8

Verify that the node is removed from the cluster.

9

Log in as the root or NSP admin user on the NSP deployer VM.

10

Open the following file using a plain-text editor such as vi:

/opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml

11

Remove all references to the removed node to ensure that the node cannot be added back into the cluster during a redeployment operation.

12

Save and close the file.

13

Create a backup copy of the updated k8s-deployer.yml file, and transfer the backup copy to a station that is separate from the NSP system, preferably in a remote facility.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14

Enter the following:

```
# cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
```

15

Enter the following to create the cluster configuration:

```
# ./nspk8sctl config -c ↵
```

The following is displayed when the creation is complete:

```
✓ Cluster hosts configuration is created at:
/opt/nsp/nsp-k8s-deployer-Release-ID/config/hosts.yml
```

16

Perform 13.4 “How do I back up the NSP cluster databases?” (p. 410) to ensure that the reconfigured cluster can be restored in the event of a failure.

17

Close the console window.

END OF STEPS

12.20 How do I change NSP system addressing?

12.20.1 Purpose

CAUTION

Service Disruption

Changing an IP address or hostname in an NSP system is a complex operation that requires careful planning and organization, and may require a complete system redeployment.

Do not attempt to modify the network configuration of an NSP component without assistance from NSP professional services.

Changing the addressing of the NSP deployer VM or NSP cluster members may be required, for example, when the management network topology changes.

The requirements of such an operation depend on the management network topology and other considerations, so must be planned, co-ordinated, and performed only under the guidance of technical support.

Note: In-service hostname modification on an NSP deployer VM or NSP cluster member is not possible. Such a modification requires a complete system reinstallation, and a reimport of the Helm charts and container images. Contact NSP technical support for more information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.20.2 Steps

1

Collect the following information:

- each NSP deployer VM, NSP cluster, and ancillary component hostname
- each NSP deployer VM, NSP cluster, and ancillary component IP address
- configuration information for mechanisms in the management network that affect addressing, such as NAT
- each proposed new IP address or hostname

2

Contact NSP professional services to plan and schedule a maintenance period for the addressing change.

END OF STEPS

12.21 How do I back up the NSP deployer VM?

12.21.1 Purpose

Perform the following steps to back up the NSP deployer VM in an NSP cluster. An NSP deployer VM backup is crucial for the recovery of the NSP deployer VM in the event of a failure.

Note: The steps describe how to back up an NSP deployer VM in a KVM virtualization environment; for OpenStack or VMware ESXi, see the RHEL or VMware documentation for information about how to restore a VM.

12.21.2 Steps

1

Open a terminal session to the NSP hypervisor VM.

2

Log in as the root or NSP admin user.

3

Enter the following to stop the VM:

```
# virsh destroy VM ↵
```

where *VM* is the VM name

4

Enter the following to convert the NSP deployer VM image in qcow2 format to conserve disk space:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# qemu-img convert -f raw -O qcow2 sparse_current_image raw_backup_
image.qcow2 ↵
```

where

sparse_current_image is the name of the current VM image in sparse format

raw_backup_image is the name to assign to the backup VM image in raw format

5

Enter the following to start the VM:

```
# virsh start VM ↵
```

where *VM* is the VM name

The VM starts.

6

Store the *raw_backup_image*.qcow2 file in a location separate from the NSP system and preferably in a remote facility.

7

Close the open console windows.

END OF STEPS

12.22 How do I restore the NSP deployer VM?

12.22.1 Purpose

The following steps describe how to restore the NSP deployer VM in an NSP cluster, for example, if the deployer VM fails and must be recreated.

Note: The steps describe how to restore an NSP deployer VM in a KVM virtualization environment; for OpenStack or VMware ESXi, see the RHEL or VMware documentation for information about how to restore a VM.

Note: In order to perform the procedure, you require a backup of the NSP deployer VM configuration. A backup is created during NSP system deployment or reconfiguration, and also by performing 12.21 “How do I back up the NSP deployer VM?” (p. 391).

12.22.2 Steps

1

Open a terminal session to the NSP hypervisor VM.

2

Log in as the root or admin user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Create a temporary local directory.

Note: The directory must be empty.

4

Enter the following:

```
# cd directory ↵
```

where *directory* is the temporary directory created in Step 3.

5

Copy the NSP deployer VM backup file set to the temporary directory.

6

Enter the following to convert the backup NSP deployer VM qcow2 image to raw format:

```
# qemu-img convert -f qcow2 backup_image.qcow2 -O raw new_image.img ↵
```

where

backup_image is the backup image file name

new_image is a name to assign to the new image file

7

If the NSP deployer VM is running, enter the following to stop the VM:

```
# virsh destroy VM ↵
```

where *VM* is the VM name

8

Enter the following to deploy the VM:

Note: One "--network bridge=*bridge_name"* entry is required for each VM interface that you intend to configure.

```
# virt-install --connect qemu:///system --ram RAM --vcpu=vCPUs -n
instance --os-type=linux --os-variant=rhel7 --disk path="new_image",
device=disk,bus=virtio,format=raw,io=native,cache=none --network
bridge=bridge_name --import & ↵
```

where

RAM is the required amount of VM RAM in the response to your Platform Sizing Request, in Mbytes; for example, 64 Gbytes is expressed as 65536, which is 64 x 1024 Mbytes

vCPUs is the required number of vCPU threads in the response to your Platform Sizing Request

instance is the name to assign to the VM

new_image is the name of the disk image created in Step 6

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

bridge_name is the name of the network bridge for a VM interface

9

When the VM creation is complete, enter the following:

```
# virsh domiflist deployer_host | awk '{print $5}' ↵
```

where *deployer_host* is the instance name assigned to the VM

The NSP deployer VM MAC address is displayed.

10

Record the MAC address for use in a later step.

11

Enter the following to open a console session as the root user on the NSP deployer VM:

```
# virsh console deployer_host ↵
```

12

Open the following file with a plain-text editor such as vi:

/etc/sysconfig/network-scripts/ifcfg-eth*n*

where

n is the Ethernet interface number; for example, eth0 is the first interface

13

Edit the following line as shown below:

```
HWADDR=MAC_address
```

where *MAC_address* is MAC address recorded in Step 9

14

Save and close the file.

15

Enter the following:

```
# init 6 ↵
```

The NSP deployer VM reboots, and the NSP deployer VM is restored.

16

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12.23 How do I replace an NSP cluster node?

12.23.1 Purpose

The following steps describe how to replace a node in an NSP cluster, as may be required in the event of a node failure.

Note: If root access for remote operations is disabled in the NSP configuration, remote operations such as SSH and SCP as the root user are not permitted within an NSP cluster. Steps that describe such an operation as the root user must be performed as the designated non-root user with sudoer privileges.

For simplicity, such steps describe only root-user access.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

Node replacement in a standalone deployment

In order to perform the procedure in a standalone NSP deployment, the following must be true.

- Scheduled NSP backups are enabled, as described in Chapter 22, “Classic management database administration”.
- A recent NSP system backup is available.

Note: If you need to replace a node in a standalone NSP cluster and do not have a recent NSP system backup, you cannot use the procedure to replace the node. Instead, you must recreate the cluster configuration; contact technical support for assistance.

CAUTION

Service outage

Performing the procedure in a standalone NSP deployment causes a service outage.

Ensure that you perform the procedure only during a scheduled maintenance period with the supervision of Nokia technical support.

12.23.2 Steps

Acquire node information

1

Log in as the root or NSP admin user on the NSP cluster host in the NSP cluster that requires the node replacement.

2

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Open a console window.

3

Enter the following to show the node roles:

```
# kubectl get nodes --show-kind ↵
```

Output like the following is displayed; the example below is for a three-node cluster:

```
NAME          STATUS   ROLES                  AGE   VERSION
node/node1    Ready    control-plane,master   18d   v1.20.7
node/node2    Ready    control-plane,master   18d   v1.20.7
node/node3    Ready    <none>                 18d   v1.20.7
```

If the Roles value for the node you are replacing includes control-plane or master, the node has a master role; if the value is <none>, the node is a worker node.

4

Enter the following to show the node labels:

```
# kubectl get nodes --show-labels ↵
```

```
NAME    STATUS   ROLES           AGE   VERSION   LABELS
node1   Ready    control-plane   10d   v1.32.5   beta.kubernetes.
io/arch=amd64,beta.kubernetes.io/os=linux,etcd=true,isIngress=true,
kubernetes.io/arch=amd64,kubernetes.io/hostname=test-node1,kubernetes.
io/os=linux,node-role.kubernetes.io/control-plane=,node.kubernetes.
io/exclude-from-external-load-balancers=

node2   Ready    control-plane   10d   v1.32.5   beta.kubernetes.
io/arch=amd64,beta.kubernetes.io/os=linux,etcd=true,isIngress=true,
kafka-0=true,kafka=true,kubernetes.io/arch=amd64,kubernetes.
io/hostname=test-node2,kubernetes.io/os=linux,node-role.kubernetes.
io/control-plane=,node.kubernetes.
io/exclude-from-external-load-balancers=

node3   Ready    <none>          10d   v1.32.5   beta.kubernetes.
io/arch=amd64,beta.kubernetes.io/os=linux,etcd=true,file-service=true,
isIngress=true,kubernetes.io/arch=amd64,kubernetes.io/hostname=node3,
kubernetes.io/os=linux,linbit.com/hostname=node3,storage=true

node4   Ready    <none>          10d   v1.32.5   beta.kubernetes.
io/arch=amd64,beta.kubernetes.io/os=linux,isIngress=true,kubernetes.
io/arch=amd64,kubernetes.io/hostname=node4,kubernetes.io/os=linux,
linbit.com/hostname=node4,storage=true

node5   Ready    <none>          10d   v1.32.5   beta.kubernetes.
io/arch=amd64,beta.kubernetes.io/os=linux,isIngress=true,kubernetes.
io/arch=amd64,kubernetes.io/hostname=node5,kubernetes.io/os=linux,
linbit.com/hostname=node5,storage=true
```

The storage=true label applies only to a multi-node setup as follows:

- If an NSP cluster has more than three nodes, by default, the last three nodes are used to set the storage label.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- You can set the storage label for a dedicated node.

  If the NSP cluster has more than three nodes and you want to set the label on nodes other than last three nodes, set the label on a dedicated node as follows before performing Step 13:

  # **kubectl label node *node* storage=true**

  where node is name of the dedicated node
- For two-node and three- node NSP setups, Step 13 sets storage=true on all nodes.

Ensure correct DR cluster roles

5

If the NSP system is not a DR deployment, skip this step.

In order to replace an NSP cluster node, the node must be in the standby cluster. After the failure of an DR NSP cluster node that hosts an essential NSP service, an NSP switchover automatically occurs. However, no automatic switchover occurs for a node that does not host an essential service.

If the node to replace is currently in the primary NSP cluster, perform 15.4 “How do I perform an NSP DR switchover from the NSP UI?” (p. 453).

Stop NSP cluster

6

Stop the NSP cluster.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass uninstall --undeploy

Note: In a standalone deployment, performing this step marks the beginning of the service outage.

1. Open a terminal session to the NSP deployer VM.
2. Log in as the root or NSP admin user.
3. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
4. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```
5. Save and close the file.
6. Enter the following:

   # **cd /opt/nsp/NSP-CN-DEP-*release-ID*/bin** ↵
7. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ./nspdeployerctl uninstall --undeploy ↵
```

The NSP cluster stops.

Reconfigure and start cluster

7

If the replacement node has the same IP address as the node you are replacing, you can skip this step.

Update the node IP address in the NSP cluster configuration.

1. Open the following file on the NSP deployer VM using a plain-text editor such as vi:

   /opt/nsp/nsp-k8s-deployer-*release-ID*/config/k8s-deployer.yml
2. Change the former node IP address to the new IP address.
3. Save and close the file.
4. Enter the following:

   ```
   # cd /opt/nsp/nsp-k8s-deployer-release-ID/bin ↵
   ```
5. Enter the following:

   ```
   # ./nspk8sctl config -c ↵
   ```

   A new /opt/nsp/nsp-k8s-deployer-*release-ID*/config/hosts.yml file is created.

8

Enter the following:

```
# ssh-copy-id -i ~/.ssh/id_rsa.pub root@address ↵
```

where *address* is the replacement node IP address

The required SSH key is transferred to the replacement node.

9

Perform the following steps to back up the Kubernetes secrets.

1. Enter the following on the NSP deployer VM:

   ```
   # cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
   ```
2. Enter the following:

   ```
   # ./nspdeployerctl secret -o backup_file backup ↵
   ```

   where *backup_file* is the absolute path and name of the backup file to create

   As the secrets are backed up, messages like the following are displayed for each Kubernetes namespace:

   ```
   Backing up secrets to /opt/backupfile...
     Including secret namespace:ca-key-pair-external
     Including secret namespace:ca-key-pair-internal
     Including secret namespace:nsp-tls-store-pass
   ```

   When the backup is complete, the following prompt is displayed:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Please provide an encryption password for backup_file
enter aes-256-ctr encryption password:
```

3. Enter a password.

   The following prompt is displayed:

   ```
   Verifying - enter aes-256-ctr encryption password:
   ```

4. Re-enter the password.

   The backup file is encrypted using the password.

5. Record the password for use when restoring the backup.
6. Record the name of the data center associated with the backup.
7. Transfer the backup file to a secure location in a separate facility for safekeeping.

10

Enter the following:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
`nspk8sctl --ask-pass uninstall`

```
# ./nspk8sctl uninstall ↵
```

The Kubernetes software in the cluster is uninstalled.

11

Perform the following steps to restore the NSP Kubernetes secrets.

1. Enter the following on the NSP deployer VM:

   ```
   # cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
   ```

2. Enter the following:

   ```
   # ./nspdeployerctl secret -i backup_file restore ↵
   ```

   where *backup_file* is the absolute path and filename of the secrets backup file created in Step 9

   The following prompt is displayed:

   ```
   Please provide the encryption password for /opt/backupfile
   enter aes-256-ctr decryption password:
   ```

3. Enter the password recorded during the backup creation.

   As the secrets are restored, messages like the following are displayed for each Kubernetes namespace:

   ```
   Restoring secrets from backup_file...
   secret/ca-key-pair-external created
     Restored secret namespace:ca-key-pair-external
   secret/ca-key-pair-internal created
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
  Restored secret namespace:ca-key-pair-internal
secret/nsp-tls-store-pass created
  Restored secret namespace:nsp-tls-store-pass
```

12

Enter the following:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspk8sctl --ask-pass install

```
# ./nspk8sctl install ↵
```

The Kubernetes software in the cluster is re-installed.

13

Add the labels from the former node to the replacement node.

1. Enter the following:

   ```
   # cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
   ```

2. Enter the following:

   ```
   # ./nspdeployerctl config ↵
   ```

3. On the NSP cluster host, enter the following:

   ```
   # kubectl get nodes node --show-labels ↵
   ```

   where *node* is the node name

4. Verify that the labels match the labels recorded in Step 4.

14

Update the node IP address in the NSP software configuration file.

1. Open the following file on the NSP deployer VM using a plain-text editor such as vi:
   /opt/nsp/NSP-CN--DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
2. If the former node IP address is present in the file, replace it with the new IP address.
3. Save and close the file.

15

Enter the following on the NSP deployer VM:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config ↵
```

The new node IP address is propagated to the deployment configuration.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16

Perform one of the following.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --deploy

a. If the NSP is deployed in a DR configuration, enter the following on the standby NSP deployer VM:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --deploy
↵
```

The NSP starts.

b. If the NSP system is configured as an enhanced deployment without DR, you must ensure that the PostgreSQL and Neo4j databases in the cluster initialize on an existing node, and not on the replacement node, by cordoning the replacement node until after the initialization.

1. Enter the following on the NSP cluster host:

   ```
   # kubectl cordon node ↵
   ```

   where *node* is the node name

   The replacement node is cordoned.

2. On the NSP deployer VM, enter the following:

   ```
   # /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install
   --deploy ↵
   ```

3. On the NSP cluster host, enter the following:

   ```
   # kubectl get pods -A ↵
   ```

   The pods are listed.

4. View the output; if all of the following are not true, repeat 3.

   Note: You must not proceed to the next step until the conditions are met.
   - One postgres-primary pod instance is in the Running state.
   - At least two nspos-neo4j-core pod instances are in the Running state.
   - At least two nsp-tomcat pod instances are in the Running state.
   - If nrcx-tomcat is installed, at least two nrcx-tomcat pods are in the Running state.

5. When the conditions are met, enter the following:

   ```
   # kubectl uncordon node ↵
   ```

   The replacement node is uncordoned.

c. If the node to be replaced is not in a DR or enhanced deployment, skip this step.

Perform 13.7 “How do I restore the NSP cluster databases?” (p. 417) using a copy of the appropriate NSP system backup, which is typically the most recent.

Note: Do not perform Step 4, which deletes all databases.

Note: The restore procedure starts the NSP cluster when the restore is complete.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17

Back up the NSP cluster data, as described in 13.4 “How do I back up the NSP cluster databases?” (p. 410).

18

Close the open console windows.

END OF STEPS

12.24 How do I restore the NSP OpenSearch log data?

12.24.1 Purpose

Perform this procedure to restore legacy NSP OpenSearch log data from a backup.

Note: If the kubeconfig files in /opt/nsp/nsp-configurator/kubeconfig on the NSP deployer host contain an expired certificate, enter the following command to resynchronize the kubeconfig files from the NSP cluster; see 7.7 “How do I update nsp_kubeconfig on the NSP deployer host?” (p. 119).

```
# ./nspk8sctl update --kubeconfig ↵
```

The nsp-log-collector tool is run from the Deployer VM.

12.24.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer VM.

2

Open a console window.

3

Navigate to the log collector directory and extract the archive:

```
# cd
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/support/logCollector/
↵
```

4

Enter the following:

```
# unzip nsp-log-collector.zip ↵
```

The following files are created in the current directory:

- nsp-log-collector
- README.txt

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

After the files are extracted, enter the following:

```
# cd
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/support/logCollector/nsp-
↵
```

6

Enter the following to back up all collected OpenSearch log data:

```
# ./nsp-log-collector.sh --postAll backup_file ↵
```

where *backup_file* is the absolute path of the backup file

The log data files are extracted to the specified location.

7

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13 NSP cluster database administration

13.1 How do I check NSP database synchronization?

13.1.1 Purpose

Perform this procedure to check the synchronization status of the database instances in the redundant NSP clusters of a DR deployment. You can check the synchronization status from the NSP GUI, or using a CLI.

13.1.2 Steps

Check database synchronization from the NSP GUI

1

As an NSP administrator, choose **System Health** from the NSP main menu.

2

In the System Health dashboard, click **Expand Size** on the Database Synchronization Status dashlet.

3

View the information in the expanded Database Synchronization Status list.

The **Sync Status** column displays the synchronization completion percentage for each of the database pods. If the Sync Status for a database is less than 99%, it is generally not safe to switch between databases, although system load is also a factor. Consider whether the system is currently under heavy load or if there are networking issues between clusters, as these factors could contribute to reduced synchronization. A Sync Status of 97-98% is acceptable on systems with high load.

If the **In Recovery** or **Replay Paused** columns are True, it is not safe to switch.

END OF STEPS

13.1.3 Steps

Check database synchronization using a CLI

1

Log in as the root or NSP admin user on the NSP cluster host in the primary data center.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm/ {print
$1;exit}') -it $(kubectl get pods -A| awk '/nspos-asm/ {print
$2;exit}') -c nspos-asm-app -- /bin/bash -c 'source ~/.bashrc &&
/opt/nsp/os/asm/bin/report.py' ↵
```

4

Database synchronization data is returned for all NSP database instances in tabular format, with information presented under the following columns:

- `dcName` - string value
- `dbName` - string value (postgres | neo4j)
- `podName` - string value
- `role` - string value (PRIMARY | STANDBY for postgres, LEADER | FOLLOWER | READ_REPLICA for neo4j)
- `activeSize` - string value
- `sizeUnit` - string value (Bytes for postgres, Commits for neo4j)
- `isInRecovery` - null (or boolean for postgres)
- `isReplayPaused` - null (or boolean for postgres)
- `receivedSize` - null (or string for postgres)
- `replaySize` - null (or string for non primary/leader instances)
- `lastReplayTimeStamp` - null (or timestamp string for postgres)
- `missingSize` - null (or string for non primary pg instances)
- `dataToTransfer` - null (or string for non primary pg instances)
- `dataToProcess` - null (or string for non primary/leader instances)
- `syncPercentage` - double (real number 0-100)

5

Review the information.

If “syncPercentage” for a database is less than 99%, it is generally not safe to switch between databases, although system load is also a factor. Consider whether the system is currently under heavy load or if there are networking issues between clusters, as these factors could contribute to reduced synchronization. A “syncPercentage” of 97-98% is acceptable on systems with high load.

If “isInRecovery” or “isReplayPaused” are True, it is not safe to switch.

6

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13.2 What do I need to know about backing up and restoring NSP cluster data?

13.2.1 Introduction

The procedures in the following sections describe how to back up and restore the system data and application databases of an NSP cluster.

Note: The following RHEL CLI prompts in command lines denote the active user, and are not to be included in typed commands:

- #—root user
- bash$—nsp user

Note: NSP Analytics data, such as the report repository contents, are stored in the PostgreSQL database, so are included in the database backup and restore operations described; no separate backup or restore process is required for Analytics data.

Integrated deployments

In an NSP system that has integrated components such as the NFM-P or WS-NOC, it is strongly recommended that you synchronize the backup and restore operations among the components. See the WS-NOC backup and restore documentation, and Chapter 22, “Classic management database administration”, as required.

NSP database failure alarms

The NSP raises the following alarms in the event of a suspected PostgreSQL database failure:

Note: The alarms are not auto-clearing, so must be cleared manually.

- Critical—the leader database is unresponsive
- Major—at least one follower database is unresponsive

Identifying the source of a database alarm

The NSP and an integrated NFM-P raise similar alarms in response to a database failure.

Before you take action to respond to a database alarm, you must clearly identify the system raising the alarm and the database instance at fault.

The Source Type field of a database failure alarm indicates whether the alarm source is the NSP or NFM-P.

The Site ID and Site Name fields identify the following:

- NFM-P alarm—the NFM-P main server that raised the alarm
- NSP alarm—the faulty PostgreSQL database instance

Note: Regardless of the source system, the Additional Text field contains the IP address of the database instance that is at fault.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

For example, the Source Type field of a standby database failure alarm contains “NFM-P”. An operator views the Site Name field, which identifies the NFM-P main server that has reported the fault. The operator then views the Additional Text field, and learns that the standby database associated with the main server has failed.

When a similar NSP alarm is raised, the operator has to view only the Site ID or Site Name field to identify which PostgreSQL database instance is at fault.

13.3 How do I configure scheduled NSP backups?

13.3.1 Purpose

Perform this procedure to configure scheduled backups of the following NSP cluster databases:

- Kubernetes etcd data
- NSP file service data
- PostgreSQL
- nspos-solr
- nsp-tomcat
- nrcx-tomcat
- OpenSearch

Note: In the above list, backup of the OpenSearch database refers to backup and restore of configured data where the data is configured by the user or already available in the OpenSearch cluster. It is not related to log data in 12.24 “How do I restore the NSP OpenSearch log data?” (p. 402).

Scheduled backups are enabled by default, and scheduled to run daily at 12:30 AM UTC.

Note: By default, the NSP retains the three most recent scheduled backups.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

13.3.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer VM.

2

Open the following file with a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Locate the section that begins with the following:

```
backups:
```

4

Configure the following parameters:

Note: If the schedule value is an empty string, no scheduled backup is performed.

Note: See the RHEL cron man page for information about defining a crontab schedule.

```
schedule: "definition"
retained: n
```

where

definition is a UNIX crontab schedule definition; for example, “30 0 * * *” specifies the default backup schedule of 12:30 a.m. daily

n is the number of backups to retain

5

Save and close the file.

6

If the database is large and you have the required storage to store the PostgreSQLdatabase in intermediate files, perform the following to reduce the PostgreSQL backup duration.

a. Log in as the root user on the NSP cluster host that is a Kubernetes control-plane node in the Kubernetes cluster.

b. Open a console window.

c. Enter the following to configure the USEBASEBACKUP parameter in nspos-postgresql-configmap:

```
# kubectl edit configmap nspos-postgresql-configmap -n
nsp-psa-restricted
```

The file opens in a plain-text editor such as vi.

d. Locate the section that begins with the following:

```
pg_backup.conf:
```

e. Configure the following:

```
USEBASEBACKUP:true
```

f. Save and close the file.

In the next scheduled backup, the system uses the optimized backup method.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13.4 How do I back up the NSP cluster databases?

13.4.1 Purpose

Perform this procedure to manually create a backup of one or more of the following in an NSP cluster:

- Kubernetes etcd data
- NSP Kubernetes secrets
- NSP file service data
- PostgreSQL
- nspos-solr
- nsp-tomcat
- nrcx-tomcat
- OpenSearch

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

13.4.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

If a common backup storage location is defined in the NSP configuration, go to Step 7.

4

Open the following file with a plain-text editor such as vi:
/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

5

Configure the backups to be stored on an NFS server.

1. Locate the section that begins with the following:

   ```
   backups:
   ```

2. Configure the following parameters in the following subsection:

   ```
           nfs:
   ```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
server: "server"
path: "path"
```

where

server is the NFS server IP address

path is the path of the exported file system on the server

Note: If there are pre-existing nsp-backup-storage PVC (and associated PV) configured, they must be deleted before applying the new configuration.

6

Enter the following command to apply the nsp-config.yml changes to the cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config --deploy

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

Note: If the kubeconfig files in /opt/nsp/nsp-configurator/kubeconfig on the NSP deployer host contain an expired certificate, enter the following command to resynchronize the kubeconfig files from the NSP cluster; see 7.7 “How do I update nsp_kubeconfig on the NSP deployer host?” (p. 119).

```
# ./nspk8sctl update --kubeconfig ↵
```

7

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
```

8

Enter one or more of the following, as required, to back up system data and databases:

Note: It is recommended that you back up all system data and databases.
You must not proceed to the next step until each backup job is complete.
The system performs the backup of the index detail and user-related configured data in OpenSearch, such as dashboard, saved OpenSearch filters, visualise and other data configured by the user. The backup of the logs is available through the logCollector tool.

a. To back up the NSP Kubernetes etcd data:

```
# ./nspos-db-backup-k8s.sh nsp-etcd backup_dir ↵
```

b. To back up the NSP file service data:

```
# ./nspos-db-backup-k8s.sh nsp-file-service backup_dir ↵
```

c. To back up the NSP PostgreSQL database:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ./nspos-db-backup-k8s.sh nspos-postgresql backup_dir ↵
```

d. To back up the NSP Solr database:

```
# ./nspos-db-backup-k8s.sh nspos-solr backup_dir ↵
```

e. To back up the NSP Tomcat database:

```
# ./nspos-db-backup-k8s.sh nsp-tomcat backup_dir ↵
```

f. To back up the cross-domain Tomcat database:

```
# ./nspos-db-backup-k8s.sh nrcx-tomcat backup_dir ↵
```

g. To back up the OpenSearch database:

```
# ./nspos-db-backup-k8s.sh opensearch backup_dir ↵
```

where *backup_dir* is the directory in which to store the backup

The backup script displays messages like the following as a backup job proceeds:

```
---------------- BEGIN : Backing up database-backup ----------------
job.batch/backup_job created
timestamp LOG: Waiting for job backup_job at namespace namespace to
finish...
timestamp LOG: backup done successfully
timestamp LOG: Removing job backup_job at namespace namespace
job.batch "backup_job" deleted
timestamp LOG: Job backup_job at namespace namespace deleted
---------------- END : Backing up database_backup ----------------
---------------- BEGIN : Fetching backup database ----------------
timestamp LOG: Fetching database backup from pod nsp-backup-storage-0
at namespace namespace
timestamp LOG: Latest database backup is database_backup_timestamp.
tar.gz
tar: removing leading '/' from member names
timestamp LOG: Latest database backup fetched successfully
---------------- END : Fetching backup database ------------------
```

A backup filename has the following format:

*database*_backup_*timestamp*.tar.gz

where

database is the database name, for example, nspos-tomcat

timestamp is the start time of the database backup

Note: This step applies only starting with Release 25.8. The OpenSearch database is excluded from the backup operation if the system has been upgraded from a release earlier than Release 25.8.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Safeguard backup files

9

Transfer the files in *backup_dir* to a secure location for safekeeping.

Note: It is strongly recommended that you transfer each backup file to a secure facility that is outside the local data center.

10

Close the console window.

END OF STEPS

13.5 How do I retrieve cluster database backup files?

13.5.1 Purpose

Perform this procedure to locate and retrieve NSP cluster database backup files.

13.5.2 Steps

1

Open a terminal session to the NSP master node (typically node1).

2

Log in as the root or NSP admin user.

3

List available backup files for a cluster:

```
# kubectl exec -n nsp-psa-restricted nsp-backup-storage-0 -- ls
/tmp/backups
```

The system returns a list of backups.

4

Copy the name of the most recent backup and then run the following command to copy it to a backup directory on the master node:

```
# kubectl cp -n nsp-psa-restricted nsp-backup-storage-0:
/tmp/backups/backup_name /opt/nsp/backups/
```

where

- *backup_name* is the NSP backup file you are retrieving, eg. **nsp-tomcat**. If you want to retrieve a specific backup set, specify a backup file name. Otherwise, you can retrieve the entire **/tmp/backups** directory contents.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- **/opt/nsp/backups/** is the target location of the copied backup file(s). You can specify a different location.

5

Close the console window.

END OF STEPS

13.6 How do I restore the Kubernetes etcd data in an NSP cluster?

13.6.1 Purpose



CAUTION

System Data Corruption

Attempting to restore the etcd data from one NSP cluster to a different NSP cluster causes the restore to fail, and renders the NSP cluster unrecoverable.

You must restore only an etcd data backup from the same NSP cluster; you cannot move an NSP cluster configuration to a different cluster, or restore a cluster configuration in a new cluster.

An etcd data backup, called a snapshot, captures all Kubernetes objects and associated critical information. A scheduled etcd data snapshot is performed daily. The following procedure describes how to recover a failed NSP cluster by restoring the etcd data from a snapshot.

13.6.2 Steps

Obtain and distribute snapshot

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Enter the following to identify the namespace of the nsp-backup-storage pod:

```
# kubectl get pods -A | grep nsp-backup ↵
```

The leftmost entry in the output line is the namespace, which in the following example is nsp-psa-restricted:

```
nsp-psa-restricted   nsp-backup-storage-0   1/1   Running   0   5h16m
```

3

Record the namespace value.

4

Enter the following to identify the etcd snapshot to restore:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# kubectl exec -n namespace nsp-backup-storage-0 - ls -la
/tmp/backups/nsp-etcd/ ↵
```

where *namespace* is the namespace value recorded in Step 3

The directory contents are listed; the filename format of an etcd snapshot is:

nsp-etcd_backup_*timestamp*.tar.gz

where *timestamp* is the snapshot creation time

5

Record the name of the snapshot file that you need to restore.

6

Enter the following to copy the snapshot file from the backup pod to an empty directory on the local file system:

```
# kubectl cp namespace/nsp-backup-storage-0:
/tmp/backups/nsp-etcd/snapshot_file path/snapshot_file ↵
```

where

namespace is the namespace value recorded in Step 3

path is an empty local directory

snapshot_file is the snapshot file name recorded in Step 5

7

Enter the following:

Note: The file lists either one member, or three, depending on the deployment type.

```
# grep ETCD_INITIAL /etc/etcd.env ↵
```

Output like the following is displayed.

```
ETCD_INITIAL_ADVERTISE_PEER_URLS=https://local_address:port
ETCD_INITIAL_CLUSTER_STATE=existing
ETCD_INITIAL_CLUSTER_TOKEN=k8s_etcd
ETCD_INITIAL_CLUSTER=etcd1=https://address_1:port,etcd2=https:
//address_2:port,etcd3=https://address_3:port
```

where

local_address is the IP address of the etcd cluster member you are operating from

address_1. *address_2*. and *address_3* are the addresses of all etcd cluster members

port is a port number

8

Perform the following on each etcd cluster member.

Note: After this step, the etcd cluster is unreachable until the restore is complete.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Log in as the root or NSP admin user.
2. Enter the following:

   # **systemctl stop etcd** ↵

   The etcd service stops.
3. Transfer the snapshot file obtained in Step 7 to the cluster member.

Restore database on etcd cluster members

9

Perform Step 11 to Step 19 on each etcd cluster member.

10

Go to Step 20.

11

Log in as the root or NSP admin user.

12

Navigate to the directory that contains the transferred snapshot file.

13

Enter the following:

tar xzf *path*/nsp-etcd_backup_*timestamp*.tar.gz ↵

where

path is the absolute path of the snapshot file

timestamp is the snapshot creation time

The snapshot file is uncompressed.

14

Enter the following:

ETCDCTL_API=3 etcdctl snapshot restore etcd.db --name *member* --initial-cluster *initial_cluster* --initial-cluster-token *token* --initial-advertise-peer-urls *URL* ↵

where

member is the name of the cluster member you are working on, for example, etcd2

initial_cluster is the ETCD_INITIAL_CLUSTER list of cluster members recorded in Step 7

token is the ETCD_INITIAL_CLUSTER_TOKEN value recorded in Step 7

URL is the URL of the cluster member you are working on; for example, the etcd2 cluster member URL shown in Step 7 is https://*address_2*:*port*

The etcd database is restored.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

15

Enter the following to create a directory in which to store the previous database:

```
# mkdir path/old_etcd_db ↵
```

where *path* is the absolute path of the directory to create

16

Enter the following to move the previous database files to the created directory:

```
# mv /var/lib/etcd/* path/old_etcd_db ↵
```

where *path* is the absolute path of the directory created in Step 15

17

Enter the following:

```
# mv ./member.etcd/* /var/lib/etcd/ ↵
```

where *member* is the member name specified in Step 14

The backup files move to the /var/lib/etcd directory.

18

Enter the following:

```
# systemctl start etcd ↵
```

The etcd service starts.

19

Enter the following:

```
# systemctl status etcd ↵
```

The etcd service status is displayed.

The service is up if the following is displayed:

```
Active: active (running)
```

20

When the etcd service is up, close the open console windows.

END OF STEPS

13.7 How do I restore the NSP cluster databases?

13.7.1 Purpose

Perform this procedure to restore one or more of the following in each NSP cluster:

- NSP Kubernetes secrets
- NSP file service data
- PostgreSQL database

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- nspos-solr database
- nsp-tomcat database
- nrcx-tomcat database
- OpenSearch database

Note: The nsp-tomcat and nrcx-tomcat database backup files are each named graph.db. You must ensure that you are using the correct graph.db backup file when you restore the nsp-tomcat or nrcx-tomcat database.

Note: If you are performing the procedure as part of a system conversion, migration, or upgrade procedure in a DR deployment, you must perform the procedure only in the new primary NSP cluster.

Note: You can specify a local backup file path, or a remote path, if the remote server is reachable from the NSP deployer VM and from the NSP cluster host.

To specify a remote path, use the following format for the *backup_file* parameter in the command, where *user* has access to *backup_file* at the *server* address:

`user@server:/backup_file`

Note: If root access for remote operations is disabled in the NSP configuration, remote operations such as SSH and SCP as the root user are not permitted within an NSP cluster. Steps that describe such an operation as the root user must be performed as the designated non-root user with sudoer privileges.

For simplicity, such steps describe only root-user access.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

13.7.2 Steps

Prepare to restore databases

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

If you are restoring the data on new NSP cluster VMs, create and distribute an SSH key for password-free NSP deployer VM access to each NSP cluster VM.

1. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ssh-keygen -N "" -f path -t rsa ↵
```

where *path* is the SSH key file path, for example, /home/*user*/.ssh/id_rsa

An SSH key is generated.

2. Enter the following for each NSP cluster VM to distribute the key to the VM.

```
# ssh-copy-id -i key_file user@address ↵
```

where

user is the designated NSP ansible user, if root-user access is restricted; otherwise, *user*@ is not required

key_file is the SSH key file, for example, /home/*user*/.ssh/id_rsa.pub

address is the NSP cluster VM IP address

4

Perform one of the following.

Note: You must not proceed to the next step until the cluster is ready.

a. If both of the following are true, you must stop each cluster and remove all existing cluster data:
   - You are restoring the data in an existing NSP cluster, rather than on new NSP cluster VMs.
   - You are restoring all NSP databases.

   Perform the following steps on the NSP deployer VM in each NSP cluster.

   Note: In a DR deployment, you must perform the steps first on the standby cluster.

   1. Log in as the root or NSP admin user.
   2. Open the following file with a plain-text editor such as vi:

      /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
   3. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

      ```
      deleteOnUndeploy:true
      ```
   4. Save and close the file.
   5. Enter the following:

      ```
      # cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
      ```
   6. Enter the following:

      ```
      # ./nspdeployerctl uninstall --undeploy ↵
      ```

      The NSP cluster is undeployed, and the existing data is removed.

b. If you are not restoring all databases, you must delete only the existing data in each database that you are restoring.

   Perform the following steps on the NSP deployer VM in each NSP cluster.

   Note: In a DR deployment, you must perform the steps on the NSP cluster that you want to start as the primary cluster.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Log in as the root or NSP admin user.
2. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
3. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```
4. Save and close the file.
5. On the NSP cluster host, enter the following to determine which node has the database files are:

   # **kubectl get pods -o wide -A | grep *pod* | awk '{print $8}'** ↵

   where *pod* is the pod name
6. Log in on the NSP cluster node where the pod is scheduled.
7. On the node, enter the following for each database that you are restoring:

   # **rm -rf /opt/nsp/volumes/local-provisioner/*directory*/*** ↵

   where *directory* is the directory name that includes the PVC name associated with the pod. The directory contains the database for respective pod and is one of the following:
   - nspos-solr
   - nsp-tomcat
   - nrcx-tomcat
   - opensearch-cluster-master

   For example, if the pod name is nspos-solr-statefulset-0:
   - The corresponding pvc name is solr-pvc-nspos-solr-statefulset-0
   - The corresponding directory is pvc-af7c8e88-1a5a-47ac-ac9e-5457049f416a_nsp-psa-restricted_solr-pvc-nspos-solr-statefulset-0
   - The PV name is pvc-af7c8e88-1a5a-47ac-ac9e-5457049f416a

   To delete the nsp-file-service database on a multi-node deployment:
   a. Log in to the nfs-server pod.
   b. Enter the following command from node 1 to log in to the nfs-server pod:

      # kubectl exec -it *nfs_server_pod* -n nsp-psa-privileged -- bash ↵

      where *nfs_server_pod* is the name of the nfs-server pod.
   c. Enter the following command to delete the nsp-file-service database:

      # **rm -rf /exports/nsp-psa-restricted-nsp-file-service-app-data/fileservice/***

   To delete the nsp-file-service database on a single-node deployment:
   a. Log in to the nsp-file-service-app pod.
   b. Enter the following command from node 1 to log in to the nsp-file-service-app pod:

      # kubectl exec -it *nsp_file_service_app_pod* -n nsp-psa-restricted -- bash ↵

      where *nsp_file_service_app_pod* is the name of the nsp-file-service-app pod.
   c. Enter the following command to delete the nsp-file-service database:

      # **rm -rf /opt/nsp/containers/nspvolume/fileservice/***

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

c. If both of the following are true, you must delete the existing data from the PostgreSQL database:

- The PostgreSQL database was deployed in a DR configuration. These steps should only be executed on the standby site, and not on a standalone system or on an active site.
- The deleteOnUndeploy parameter was set to ‘false’.

Perform the following:

1. Log in as the root or NSP admin user on the stanbdy deployer VM.
2. Open the following file with a plain-text editor, such as vi: /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml.
3. Verify the following line exists in the **platform** section, **kubernetes** subsection: `deleteOnUndeploy: false`.
4. Save and close the file.
5. Enter the following: **# cd /opt/nsp/NSP-CN-DEP-release-ID/bin**.
6. Enter the following: **# ./nspdeployerctl uninstall --undeploy**.

   The standby NSP cluster is undeployed.
7. Enter the following: **# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database**.
8. Enter the following: **# ./nspos-db-clear-k8s.sh nspos-postgresql**.

   The PostgeSQL database is removed from the standby cluster.

Enable NSP restore mode

5

Enter the following on the NSP deployer VM:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

6

Enter the following to enter restore mode:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the example below, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl install --config --restore --ask-pass

```
# ./nspdeployerctl install --config --restore↵
```

7

Note: The nspos-solr-statefulset-*n* and opensearch-cluster-master-*n* pods are only supported starting with Release 25.8. The pods are excluded from the restore operation if the system has been upgraded from a release earlier than Release 25.8.

The following NSP cluster pods must be operational before the restore begins:

- nsp-backup-storage-*n*

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- nspos-postgresql-primary-*n*
- nsp-file-service-app-*n*
- nspos-solr-statefulset-*n*
- present only if the NSP deployment includes Path Control functions:
  - nsp-tomcat-*dc_name*-*n*
  - nrcx-tomcat-*dc_name*-*n*

  where *dc_name* is the dcName value in the cluster configuration file
- present only if the NSP Deployment enables the loggingMonitoring feature:
  - opensearch-cluster-master-*n*

Enter the following periodically to list the pods; the cluster is ready for the restore when each required pod is in the Running state:

```
# kubectl get pods -A ↵
```

8

If any required pod is not Running, return to Step 7.

Note: A restore attempt fails unless each required pod is Running.

Restore data

9

Enter the following on the NSP deployer VM:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
```

10

Enter one or more of the following, as required, to restore system data and databases:

Note: In a DR deployment, you must perform the steps first in the data center that you want to start as the primary data center.

Note: If the kubeconfig files in /opt/nsp/nsp-configurator/kubeconfig on the NSP deployer host contain an expired certificate, enter the following command to resynchronize the kubeconfig files from the NSP cluster; see 7.7 “How do I update nsp_kubeconfig on the NSP deployer host?” (p. 119).

```
# ./nspk8sctl update --kubeconfig ↵
```

a. To restore the NSP file service data:

```
# ./nspos-db-restore-k8s.sh nsp-file-service backup_dir/backup_file
↵
```

b. To restore the NSP PostgreSQL database:

```
# ./nspos-db-restore-k8s.sh nspos-postgresql backup_dir/backup_file
↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

c. To restore the NSP Solr database:

```
# ./nspos-db-restore-k8s.sh nspos-solr backup_dir/backup_file ↵
```

Note: This step applies only starting with Release 25.8. The NSP Solr database is excluded from backup and restore operations if the system has been upgraded from a release earlier than Release 25.8.

d. To restore the NSP Tomcat database:

```
# ./nspos-db-restore-k8s.sh nsp-tomcat backup_dir/backup_file ↵
```

e. To restore the cross-domain Tomcat database:

```
# ./nspos-db-restore-k8s.sh nrcx-tomcat backup_dir/backup_file ↵
```

f. To restore the OpenSearch database:

```
# ./nspos-db-restore-k8s.sh opensearch backup_dir/backup_file ↵
```

Note: This step applies only in Release 25.8 or later. The OpenSearch database is excluded from backup and restore operations if the system has been upgraded from a release earlier than Release 25.8.

where

backup_dir is the directory that contains the backup file

backup_file is the backup file name, for example:

- for PostgreSQL, the name is nspos-postgresql_backup_*timestamp*.tar.gz
- for OpenSearch, the name is opensearch-cluster-master-*n*

Start NSP clusters

11

Perform the following steps in each data center.

Note: In a DR deployment, you must perform the steps first in the data center that you want to start as the primary data center.

1. Open a terminal session to the NSP deployer VM.
2. Log in as the root or NSP admin user.
3. Open the following file with a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml
4. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```
5. Save and close the file.
6. Enter the following:

   ```
   # cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
   ```
7. On the NSP deployer VM, enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ./nspdeployerctl install --deploy ↲
```

The NSP initializes using the restored data.

8. Enter the following periodically on the NSP cluster host to display the cluster status:

```
# kubectl get pods -A ↲
```

The cluster is operational when the status of each pod is Running.

12

Close the open console windows.

END OF STEPS

13.8 How do I recover a failed nsp-tomcat database in a DR NSP deployment?

13.8.1 Purpose

Perform this procedure if you experience nsp-tomcat database inconsistencies and need to restore the database. You can restore the database without undeploying and redeploying NSP.

13.8.2 Steps

1

If the inconsistent database instance is in the primary data center, check the standby instance status.

1. Log in as the root or NSP admin user on the standby NSP cluster host.
2. Open a console window.
3. Enter the following:

```
# kubectl exec -it -n $(kubectl get pods -A | grep nsp-tomcat |
tail -1 | awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat
| egrep -v "haproxy|backup" | tail -1 | awk '{print $2}') -c
nsp-tomcat -- /opt/nsp/server/replication/bin/neo4j-admin backup
--backup-dir=/tmp/restoreData --from=nsp-tomcat-headless-svc:6363
--database=graph.db ↲
```

4. Enter the following:

```
# kubectl exec -it -n $(kubectl get pods -A | grep nsp-tomcat |
tail -1 | awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat
| egrep -v "haproxy|backup" | tail -1 | awk '{print $2}') -c
nsp-tomcat -- /opt/nsp/server/replication/bin/neo4j-admin backup
--backup-dir=/tmp/restoreData --from=nsp-tomcat-headless-svc:6363
--database=system ↲
```

2

If either command in Step 1 fails due to inconsistencies, perform 13.9 “How do I recover both failed nsp-tomcat databases in a DR NSP deployment using a database backup?” (p. 428).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

If both commands in Step 1 succeed, perform a switchover.

1. Log in as the root or NSP admin user on the standby NSP cluster host.
2. Enter the following:

   ```
   # kubectl exec -it -n $(kubectl get pods -A | awk
   '/nsp-role-manager/ {print $1}') $(kubectl get pods -A | awk
   '/nsp-role-manager/ {print $2}') -c role-manager --
   /opt/nsp/os/rolemgr/bin/rmgrctl toActive ↵
   ```

   When the switchover is complete, the standby cluster is the new primary cluster.
3. When the switchover is complete, sign in to the NSP as the admin user.
4. Verify that you can open Path Control.

   Note: You must not proceed to the next step until Path Control is available.

4

Enter the following to perform a manual backup on the new primary NSP cluster host:

```
# kubectl create job nsp-tomcat-backup-manual --from
cronjob/nsp-tomcat-backup -n $(kubectl get cronjob -A | grep
nsp-tomcat-backup | awk '{print $1}') ↵
```

5

If the backup fails due to inconsistencies, both database instances are inconsistent; perform 13.9 “How do I recover both failed nsp-tomcat databases in a DR NSP deployment using a database backup?” (p. 428).

6

Enter the following:

```
# kubectl exec nsp-backup-storage-0 -n $(kubectl get pods -A | grep
nsp-backup-storage | awk '{print $1}') -- ls /tmp/backups/nsp-tomcat/
↵
```

The backup files are listed.

7

Record the name of the most recent backup.

8

Enter the following:

```
# kubectl cp -n $(kubectl get pods -A | grep nsp-backup-storage | awk
'{print $1}') nsp-backup-storage-0:/tmp/backups/nsp-tomcat/backup_file
/tmp/backup_file ↵
```

where *backup_file* is the recorded backup file name

The backup file is copied to the temp directory on the NSP cluster host.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Enter the following:

```
# scp /tmp/backup_file address:/tmp ↵
```

where *address* is the address of the new standby NSP cluster host

The backup file is copied to the /tmp directory on the new standby NSP cluster host.

Restore database on new standby cluster

10

Log in as the root or NSP admin user on the new standby NSP cluster host.

11

Open a console window.

12

Enter the following:

```
# helm list -A | grep nsp-tomcat | awk -F' ' '{ print $10 }' ↵
```

The nsp-tomcat version is displayed.

13

Record the nsp-tomcat version.

14

Enter the following to uninstall nsp-tomcat:

```
# helm uninstall -n nsp-psa-restricted nsp-tomcat ↵
```

The nsp-tomcat uninstallation begins.

15

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep
nsp-tomcat | egrep -v backup | wc -l` ]
  do
    sleep 2
    echo "Still there..."
  done
```

The uninstallation is complete when the command prompt is displayed.

16

When the uninstallation is complete, enter the following to install nsp-tomcat:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
--version version --timeout 300s -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/restore.yaml ↵
```

where *version* is the nsp-tomcat version recorded in Step 13

nsp-tomcat is installed.

17

Enter the following:

```
# kubectl get pods -A ↵
```

The pods are listed.

18

If the nsp-tomcat pod is not running, repeat the command in Step 17.

Note: You must not proceed to the next step until nsp-tomcat is running.

19

Enter the following:

```
# cd
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database/nspos-
db-restore-k8s.sh nsp-tomcat /tmp/backup_file ↵
```

You are prompted to restore the database.

20

Respond to the prompt.

The nsp-tomcat database is restored from the backup file.

21

Enter the following to uninstall nsp-tomcat:

```
# helm uninstall -n nsp-psa-restricted nsp-tomcat ↵
```

The nsp-tomcat uninstallation begins.

Note: You must not proceed to the next step until the uninstallation is complete.

22

The nsp-tomcat uninstallation begins.

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep
nsp-tomcat | egrep -v backup | wc -l` ]
  do
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
    sleep 2
    echo "Still there..."
  done
```

The uninstallation is complete when the command prompt is displayed.

When the uninstallation is complete, enter the following:

23

When the uninstallation is complete, enter the following to install nsp-tomcat:

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
--version version --timeout 300s -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml ↵
```

where *version* is the nsp-tomcat version recorded in Step 13

nsp-tomcat is installed.

24

When the nsp-tomcat pod installation is complete, monitor the following log file in the nsp-tomcat pod to ensure that the database starts successfully:

/opt/nsp/server/replication/logs/debug.log

Back up database

25

Optionally, to confirm that the database restore is successful, perform a switchover and perform a backup to ensure that no inconsistencies remain.

26

Close the open console windows.

END OF STEPS

13.9 How do I recover both failed nsp-tomcat databases in a DR NSP deployment using a database backup?

13.9.1 Purpose

Perform this procedure to recover the nsp-tomcat database instances in a DR NSP deployment in the event that both instances have inconsistencies. You can restore the databases without undeploying and redeploying NSP.

Note: You require a previously created and useable nsp-tomcat database backup in order to perform the procedure.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13.9.2 Steps

Prepare for data recovery

1

Retrieve the required nsp-tomcat database backup.

a. If the required backup is stored in the nsp-backup-storage-0 pod, perform the following steps.
   1. Log in as the root or NSP admin user on the NSP cluster host in the cluster that has the database backup.
   2. Open a console window.
   3. Enter the following:

      # kubectl exec nsp-backup-storage-0 -n $(kubectl get pods -A | grep nsp-backup-storage | awk '{print $1}') -- ls /tmp/backups/nsp-tomcat/ ↵

      The backup files are listed.
   4. Record the name of the most recent backup.
   5. Enter the following:

      # kubectl cp -n $(kubectl get pods -A | grep nsp-backup-storage | awk '{print $1}') nsp-backup-storage-0: /tmp/backups/nsp-tomcat/*backup_file* /tmp/*backup_file* ↵

      where *backup_file* is the recorded backup file name

      The backup file is copied to the temp directory on the NSP cluster host.

b. If the required backup is from the nsp-tomcat startup:
   1. Log in as the root or NSP admin user on the NSP cluster host in the cluster that has the database backup.
   2. Open a console window.
   3. Enter the following:

      # kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 | awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v "haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- ls /opt/nsp/server/tomcat/work/replicationArchives/ ↵

      The backup files are listed.
   4. Record the name of the most recent backup.
   5. Enter the following:

      # kubectl cp -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 | awk '{print $1}') -c nsp-tomcat $(kubectl get pods -A | grep nsp-tomcat | egrep -v "haproxy|backup" | tail -1 | awk '{print $2}'):/opt/nsp/server/tomcat/work/replicationArchives/*backup_file* /tmp/*backup_file* ↵

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

where *backup_file* is the recorded backup file name

The backup file is copied to the temp directory on the NSP cluster host.

2

Copy the backup file to the NSP deployer VM in each data center.

1. Enter the following:

   # **scp /tmp/*backup_file address*:/tmp** ↵

   where *address* is the address of the local NSP deployer VM

   The backup file is copied to the /tmp directory on the NSP deployer VM.

2. Enter the following:

   # **scp /tmp/*backup_file address*:/tmp** ↵

   where *address* is the address of the NSP deployer VM in the other data center

   The backup file is copied to the /tmp directory on the NSP deployer VM in the other data center.

3

Disable the auto-switchover function to ensure that no switchover occurs during the database restoration.

Enter the following as the root or NSP admin user on the NSP cluster host in each data center:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm-app/ {print $1}') $(kubectl get pods -A | awk '/nspos-asm-app/ {print $2}') -c nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl disableAutoFailover ↵
```

4

Enter the following as the root or NSP admin user on the NSP cluster host in either data center:

```
# helm list -A | grep nsp-tomcat | awk -F' ' '{ print $10 }' ↵
```

The nsp-tomcat version is displayed.

5

Record the nsp-tomcat version.

6

Perform Step 11 to Step 22 in the primary data center.

7

Sign in to the NSP as the admin user.

8

Verify that you can open Path Control.

You must not proceed to the next step until Path Control is available.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Perform Step 11 to Step 22 in the standby data center.

10

Go to Step 23.

Restore individual cluster

11

Enter the following on the NSP cluster host to uninstall nsp-tomcat:

```
# helm uninstall -n nsp-psa-restricted nsp-tomcat ↵
```

The nsp-tomcat uninstallation begins.

12

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep
nsp-tomcat | egrep -v backup | wc -l` ]
  do
    sleep 2
    echo "Still there..."
  done
```

The uninstallation is complete when the command prompt is displayed.

13

When the uninstallation is complete, enter the following to list the cluster nodes that can host nsp-tomcat:

```
# kubectl get pods -A -o wide | grep nsp-tomcat | egrep -v backup |
egrep -v haproxy | awk '{print $8}' ↵
```

14

Enter the following command block as the root user on each node listed in Step 13 to delete the nsp-tomcat volume data directory content:

Note: The cluster-state folder may already be empty.

```
rm -rf /opt/nsp/volumes/local-provisioner/pvc-*_nsp-psa-restricted_
neo4j-data-nsp-tomcat-*/databases
rm -rf /opt/nsp/volumes/local-provisioner/pvc-*_nsp-psa-restricted_
neo4j-data-nsp-tomcat-*/cluster-state
rm -rf /opt/nsp/volumes/local-provisioner/pvc-*_nsp-psa-restricted_
neo4j-data-nsp-tomcat-*/transactions
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

15

Enter the following on the NSP cluster host to install nsp-tomcat:

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
--version version --timeout 300s -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/restore.yaml ↵
```

where *version* is the nsp-tomcat version recorded in Step 4

nsp-tomcat is installed.

16

Restore the nsp-tomcat database.

Enter the following as the root or NSP admin user on the NSP deployer VM:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database/
nspos-db-restore-k8s.sh nsp-tomcat /tmp/backup_file ↵
```

You are prompted to restore the database.

17

Respond to the prompt.

The nsp-tomcat database is restored from the backup file.

18

Enter the following on the NSP cluster host to uninstall nsp-tomcat:

```
# helm uninstall -n nsp-psa-restricted nsp-tomcat ↵
```

The nsp-tomcat uninstallation begins.

Note: You must not proceed to the next step until the uninstallation is complete.

19

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep
nsp-tomcat | egrep -v backup | wc -l` ]
  do
    sleep 2
    echo "Still there..."
  done
```

The uninstallation is complete when the command prompt is displayed.

20

When the uninstallation is complete, enter the following to install nsp-tomcat:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
--version version --timeout 300s -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml ↵
```

where *version* is the nsp-tomcat version recorded in Step 4

nsp-tomcat is installed.

21

Enter the following:

```
# kubectl get pods -A ↵
```

The pods are listed.

22

If the nsp-tomcat pod is not running, repeat the command in Step 21.

Note: You must not proceed to the next step until nsp-tomcat is running.

Enable auto-switchover

23

Enable the auto-switchover function; enter the following as the root or NSP admin user on the NSP cluster host in each data center:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm-app/ {print
$1}') $(kubectl get pods -A | awk '/nspos-asm-app/ {print $2}') -c
nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl enableAutoFailover ↵
```

Monitor database startup

24

Monitor the following log files in the nsp-tomcat pod to ensure that the database starts without error:

- primary NSP cluster host—/opt/nsp/server/tomcat/work/logs/debug.log
- standby NSP cluster host—/opt/nsp/server/replication/logs/debug.log

25

Close the open console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13.10 How do I recover both nsp-tomcat databases in a DR NSP deployment without a database backup?

13.10.1 Purpose

Perform the procedure if you have confirmed that both the active and standby sites are inconsistent and have no useable database backup to restore. You can restore the databases without undeploying and redeploying NSP.

Note: You must perform the procedure only if you have no useable database backup, either from a daily backup or from an archive created during the nsp-tomcat pod startup.

13.10.2 Steps

1

Disable the auto-switchover function to ensure that no switchover occurs during the database restoration.

Enter the following as the root or NSP admin user on the NSP cluster host in each data center:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm-app/ {print $1}') $(kubectl get pods -A | awk '/nspos-asm-app/ {print $2}') -c nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl disableAutoFailover ↵
```

2

Enter the following as the root or NSP admin user on the NSP cluster host in either data center:

```
# helm list -A | grep nsp-tomcat | awk -F' ' '{ print $10 }' ↵
```

The nsp-tomcat version is displayed.

3

Record the nsp-tomcat version.

4

Enter the following on the NSP cluster host in each data center to uninstall nsp-tomcat:

Note: You must perform the step on the standby NSP cluster host first.

```
# helm uninstall -n nsp-psa-restricted nsp-tomcat ↵
```

The nsp-tomcat uninstallation begins.

5

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep nsp-tomcat | egrep -v backup | wc -l` ]
  do
    sleep 2
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
    echo "Still there..."
  done
```

The uninstallation is complete when the command prompt is displayed.

6

When the uninstallation is complete, enter the following on the NSP cluster host in each data center to install nsp-tomcat:

Note: You must perform the step on the primary NSP cluster host first.

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
--version version --timeout 300s -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/restore.yaml ↲
```

where *version* is the nsp-tomcat version recorded in Step 3

nsp-tomcat is installed.

7

Enter the following sequence of commands to back up the nsp-tomcat database in the primary data center:

```
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat --
/opt/nsp/server/replication/bin/neo4j-admin copy--from path=
/opt/nsp/server/tomcat/work/data/databases/graph.db--to-database=
fixed.db--from-path-tx=
/opt/nsp/server/tomcat/work/data/transactions/graph.db ↲

# mkdir -p /opt/fixed-db-backup/database ↲

# kubectl exec -it -n $(kubectl get pods -A | grep nsp-tomcat | tail
-1 | awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep
-v "haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat --
mkdir /tmp/restoreData/database ↲

# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- bash
-c "cd /opt/nsp/server/tomcat/work/data/databases/; tar-czvf
/tmp/restoreData/database/fixed.db.tar.gz ./fixed.db" ↲

#  kubectl cp -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') -c nsp-tomcat $(kubectl get pods -A | grep
nsp-tomcat | egrep -v "haproxy|backup" | tail -1 | awk '{print
$2}'):/tmp/restoreData/database/fixed.db.tar.gz
/opt/fixed-db-backup/database/fixed.db.tar.gz ↲

# cd /opt/fixed-db-backup/database/ ↲

# tar -xvf ./fixed.db.tar.gz ↲
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# mv ./fixed.db ./graph.db ↵
# mkdir -p /opt/fixed-db-backup/transactions/ ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- mkdir
/tmp/restoreData/transactions ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- bash
-c "cd /opt/nsp/server/tomcat/work/data/transactions/; tar-czvf
/tmp/restoreData/transactions/fixed.db.tar.gz ./fixed.db" ↵
# kubectl cp -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') -c nsp-tomcat $(kubectl get pods -A | grep
nsp-tomcat | egrep -v "haproxy|backup" | tail -1 | awk '{print $2}'):
# cd /opt/fixed-db-backup/transactions/ ↵
# tar -xvf ./fixed.db.tar.gz ↵
# mv ./fixed.db ./graph.db ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- rm-rfd
/tmp/restoreData/database ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- rm-rfd
/tmp/restoreData/transactions ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- rm-rfd
/opt/nsp/server/tomcat/work/data/databases/fixed.db ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') $(kubectl get pods -A | grep nsp-tomcat | egrep -v
"haproxy|backup" | tail -1 | awk '{print $2}') -c nsp-tomcat -- rm-rfd
/opt/nsp/server/tomcat/work/data/transactions/fixed.db ↵
```

8

Enter the following sequence of commands on the NSP cluster host in the primary data center for each deployed nsp-tomcat pod:

```
# cd /opt/fixed-db-backup/database ↵
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') nsp-tomcat-DC_name-pod_ID -c nsp-tomcat -- mkdir
/tmp/restoreData/database ↵
# kubectl cp -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') -c nsp-tomcat nsp-tomcat-DC_name-pod_ID:
/tmp/restoreData/database/graph.db ↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') nsp-tomcat-DC_name-pod_ID -c nsp-tomcat --  rm-rf
/opt/nsp/server/tomcat/work/data/databases/graph.db ↵
```

```
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') nsp-tomcat-DC_name-pod_ID -c nsp-tomcat --
/opt/nsp/server/replication/bin/neo4j-admin restore--force--database=
graph.db--from=/tmp/restoreData/database/graph.db ↵
```

```
# cd /opt/fixed-db-backup/transactions ↵
```

```
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') nsp-tomcat-DC_name-pod_ID -c nsp-tomcat -- rm-rfd
/opt/nsp/server/tomcat/work/data/transactions/graph.db ↵
```

```
# kubectl cp -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') -c nsp-tomcat ./graph.db nsp-tomcat-DC_name-pod_ID:
/opt/nsp/server/tomcat/work/data/transactions/graph.db ↵
```

```
# kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 |
awk '{print $1}') nsp-tomcat-DC_name-pod_ID -c nsp-tomcat --  rm-rfd
/tmp/restoreData/database ↵
```

DC_name is the primary data center name

pod_ID is the nsp-tomcat pod ID

9

Enter the following on the primary NSP cluster host to uninstall nsp-tomcat:

```
# helm uninstall -n nsp-psa-restricted nsp-tomcat ↵
```

The nsp-tomcat uninstallation begins.

Note: You must not proceed to the next step until the uninstallation is complete.

10

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep
nsp-tomcat | egrep -v backup | wc -l` ]
  do
    sleep 2
    echo "Still there..."
  done
```

The uninstallation is complete when the command prompt is displayed.

11

When the uninstallation is complete, enter the following on the NSP cluster host in the primary data center to install nsp-tomcat:

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

--version *version* --timeout 300s -f /opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml ↵

where *version* is the nsp-tomcat version recorded in Step 3

nsp-tomcat is installed.

12

Enter the following:

kubectl get pods -A ↵

The pods are listed.

13

If the nsp-tomcat pod is not running, repeat the command in Step 12.

Note: You must not proceed to the next step until nsp-tomcat is running.

14

Sign in to the NSP as the admin user.

15

Verify that you can open Path Control.

You must not proceed to the next step until Path Control is available.

16

Enter the following on the standby NSP cluster host for each nsp-tomcat pod:

kubectl exec -n $(kubectl get pods -A | grep nsp-tomcat | tail -1 | awk '{print $1}') nsp-tomcat-*DC_name-pod_ID* -c nsp-tomcat -- rm -rf/opt/nsp/server/tomcat/work/data/* ↵

DC_name is the primary data center name

pod_ID is the nsp-tomcat pod ID

17

Enter the following on the standby NSP cluster host to uninstall nsp-tomcat:

helm uninstall -n nsp-psa-restricted nsp-tomcat ↵

The nsp-tomcat uninstallation begins.

Note: You must not proceed to the next step until the uninstallation is complete.

18

Enter the following command block to monitor the uninstallation:

```
while [ 0 -lt `kubectl get pods -n nsp-psa-restricted | grep
nsp-tomcat | egrep -v backup | wc -l` ]
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
do
  sleep 2
  echo "Still there..."
done
```

The uninstallation is complete when the command prompt is displayed.

19

When the uninstallation is complete, enter the following on the NSP cluster host in the standby data center to install nsp-tomcat:

```
# helm upgrade nsp-tomcat --install oci://registry.nsp.nokia.
local/nsp/charts/cn-nsp-tomcat --namespace nsp-psa-restricted
--version version --timeout 300s -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/values.yaml -f
/opt/nsp/config/helm/values/sdn/nsp-tomcat/restore.yaml ↵
```

where *version* is the nsp-tomcat version recorded in Step 3

nsp-tomcat is installed.

20

Enable the auto-switchover function; enter the following as the root or NSP admin user on the NSP cluster host in each data center:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm-app/ {print
$1}') $(kubectl get pods -A | awk '/nspos-asm-app/ {print $2}') -c
nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl enableAutoFailover ↵
```

21

Optionally, when both NSP clusters are fully operational, back up the nsp-tomcat database; enter the following on the primary NSP cluster host:

```
kubectl create job nsp-tomcat-backup-manual --from
cronjob/nsp-tomcat-backup -n $(kubectl get cronjob -A | grep
nsp-tomcat-backup | awk '{print $1}') ↵
```

The nsp-tomcat database is backed up.

22

Close the open console windows.

END OF STEPS

13.11 How do I recover nsp-tomcat databases in an HA cluster?

13.11.1 Purpose

Perform this procedure when the restart of all three nsp-tomcat instances are triggered because one of the two original instances cannot restart. The two restarted instances cannot form a cluster,

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

and the nsp-tomcat liveness probe fails, which causes the restart. You can restore the databases without undeploying and redeploying NSP.

13.11.2 Steps

1

Perform one of the following steps.

2

Fix the situation that prevented the pod from initializing successfully. See the *NSP Troubleshooting Guide* for more information.

3

Perform the following steps:

1. Shut down the nsp-tomcat instances.
2. Fix the database. See the procedures above.
3. Restart the nsp-tomcat instances,

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14 NSP logging and monitoring

14.1 What is System Health?

14.1.1 Description

The NSP System Health dashboard displays a number of system KPIs. The default view includes a graphical representation of the number of pods in each state, such as Running or Pending, for quick identification of problems. The view also lists relevant information for each pod, such as the pod uptime, host NSP cluster node, and number of pod restarts. If a pod remains in CrashLoopBackOff state, use the recovery procedure described in 12.15 “How do I recover pods in CrashLoopBackOff state?” (p. 379).

The view displays additional information in the following dashlets:

- News Feed—list of alarms with pod and alarm information
- Kubernetes Cluster Status—graphical representation of the clusters and the state of each cluster. The view also lists relevant information for each cluster and for nodes in a cluster.
- Database Backup Status—a graphical representation of databases and the state of each backup for database backups. The view displays important information such as the backup pod status, current backup status, last run time, and last successful backup.
- Auxiliary Database Clusters—a graphical representation of clusters and the state of each cluster. The view lists relevant information for each cluster and for nodes in a cluster. You can also run auxiliary database backups directly from this dashlet.

You can also invoke the following from the System Health dashboard:

- Log Viewer—local OpenSearch instance with dashboards for viewing and analyzing NSP application log data
- Grafana—local Grafana instance that draws on various data sources to provide visualizations and alerts

14.2 What are the System Health functions?

14.2.1 Monitoring NSP

From the NSP System Health dashboard, you can monitor NSP to quickly determine the overall operational quality of the system. To view more detailed information about aspects of NSP operation, you can use Grafana and NSP Log Viewer.

The Log Viewer collects, analyzes, and displays NSP application log information by invoking a local OpenSearch instance called OpenSearch Dashboards.

From the NSP System Health dashboard, you can also open a local Grafana instance.

You can also monitor auxiliary database clusters and perform a switchover operation. See 16.2.2 “Auxiliary database cluster switchover on the NSP UI” (p. 459) for more information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14.2.2 OpenSearch Dashboards and Grafana

OpenSearch Dashboards and Grafana are third-party logging and monitoring functions that are embedded to the NSP. Each function has a dashboard that displays system status and logging information.

NSP user credentials are required to view the tools. Additionally, Grafana has Admin, Editor, and Viewer roles that can be assigned through Users and System Security.

Note: OpenSearch Dashboards and Grafana are accessible only from the URLs of the active NSP cluster. You can view NSP logging and metrics only from the currently active NSP cluster.

See 14.3 “What is Log Viewer?” (p. 441) and 14.4 “What is Grafana?” (p. 443) for more information.

14.2.3 Auxiliary database backups

You can backup the auxiliary database directly from the Auxiliary Database Clusters dashlet; see 20.7 “How do I schedule auxiliary database backups?” (p. 531) and 20.8 “How do I manually backup the auxiliary database?” (p. 532).

14.3 What is Log Viewer?

14.3.1 Overview

Log Viewer is a customizable NSP tool that uses the third-party OpenSearch utility to display all NSP application logs. All NSP application logs can be viewed in a Discover or Dashboard view.

Log Viewer analyzes the logs of NSP system elements such as the following:

- NSP clusters
- Tomcat servers
- ZooKeeper registry
- Kafka messaging system
- PostgreSQL database

The displayed logs can be searched, and filtered using custom criteria, or typical criteria such as the time of receipt.

OpenSearch documentation is available from the circular icon at the top-right of the browser window.

Log Viewer access

You can open Log Viewer using the LOG VIEWER button on the System Health dashboard, or by visiting the following URL:

https://*NSP_address*/logviewer

where *NSP_address* is the NSP address for client access

Limitations

In OpenSearch Dashboards, only the following functions are supported:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Observability
  - Applications
  - Logs
  - Traces
  - Dashboards
- Management
  - Overview
  - Index Management
  - Dashboards Management
  - Dev Tools

14.4 What is Grafana?

14.4.1 Overview

Grafana displays status information and metrics for NSP system elements. The following predefined dashboards are available:

- All Node Metrics
- All Pod Metrics
- Auxdb Agent
- Etcd Cluster Overview
- Data Collection and Analysis, Visualizations
- Kafka Server
- Keycloak Metrics
- NSP CPU/Memory/Disk Usage
- NSP deployer VM Registry
- NSP General
- NSP JVM Metrics
- NSPOS Oauth2 Proxy Metrics
- Neo4j Server Dashboard
- Nginx Request Handling Performance
- ZooKeeper Server

The information displayed by each dashboard varies by information type. For example, the All Pod Metrics dashboard displays visual indicators of memory and CPU usage in addition to numeric memory-usage indicators. The NSP Pod Status dashboard displays status graphs for a variety of NSP system elements.

14.4.2 Grafana access

You can use the GRAFANA button on the System Health dashboard to open Grafana. The tool is also available at the following URL:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

https://*NSP_address*/grafana

where *NSP_address* is the public NSP address

Note: The Grafana session does not end after an inactivity timeout. You must close the Grafana session manually.

14.5 What is user activity log forwarding?

14.5.1 User activity log forwarding overview

If the forwarding of NSP user activity logs to a remote server is enabled, each NSP user action is forwarded to a remote syslog server specified in the NSP configuration during system deployment.

14.5.2 User activity syslog record format

Each generated remote syslog message for user activity has the following fields:

- timestamp
- hostname of syslog producer
- program name
- User Activity Log entry

User Activity Log syslog record example

The following is an example of an NFM-P User Activity Log record forwarded to a remote syslog server:

Note: The record is displayed as three separate sections for illustration purposes; an actual record is contiguous.

```
May 18 09:56:36 nsp-1a3 activitylogs: {"app":"Users And Security",
"clientHost":"203.0.100.5","reqMethod":"POST","addlParams":"{}",
"actionParams":[{"val":"

{\"retentionPeriod\":32,\"activityLogsMaxSize\":1000000,
\"activityLogsWarningThreshold\":95,\"activityLogsCriticalThreshold\":
100,\"activityLogsWarningPurgePercent\":5,
\"activityLogsCriticalPurgePercent\":10}

","key":"jsonRequest"}],"respCodePhrase":"OK","timeStamp":"2020/05/27
10:47:14 821 +0000","affObjs":"{}","uid":
"a0d3b09f66acb238d9f95ab1155d075e","host":"198.51.100.16","action":"set",
"time":"1590576434821","user":"admin","reqURL":"https://198.51.100.
16/activitylogs-api/rest/api/v1/activityLogs/settings/set","respCode":
"200"}
```

The fields in the example have the following values; the actionParams section, which is the second section in the example, indicates that the action involved setting user-activity log parameters:

- timestamp—May 18 09:56:36
- hostname of syslog entry producer—nsp-1a3

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- program name—activitylogs
- User Activity Log entry—remainder that begins with "app":"Users and Security"; is in JSON format, and includes the following:
  - app—source NSP function from which action performed
  - clientHost—remote hostname or IP address that invokes action
  - reqMethod—type of action performed
  - actionParams—array; contains parameters passed to action
  - addlParams—array; contains parameters or other such values not in other fields
  - respCodePhrase—human-readable action response code
  - timeStamp—time at which action completed
  - affObjs—array of affected-object attributes, for example, FDN and ID
  - uid—record ID
  - host—IP address of server on which action performed
  - action—name of action performed
  - user—username under which action performed
  - reqURL—HTTP URL of the executed HTTP request
  - respCode—action response code, in integer format

14.6 What is the syslog record format for NSP application log forwarding?

14.6.1 Introduction

The NSP can be configured to forward NSP application-log entries for various functions, as well as NFM-P server log entries, to a remote syslog server, as described in the *NSP Installation and Upgrade Guide*. The following topics describe the syslog record formats of NSP application and NFM-P server log entries.

Syslog is defined in IETF RFC5424.

NSP application log entries

Different NSP functions log different types and amounts of information. Consequently, an NSP application log entry does not have a fixed length or number of fields, so the following topic describes only the syslog record format, and not each type of record entry.

NFM-P server log entries

When NFM-P server log forwarding is enabled, the standalone or primary NFM-P main server forwards each entry written to the local EmsServer.log file to the specified syslog server.

14.6.2 NSP application syslog record format

Each syslog record for an NSP functional area has the following fields:

- timestamp
- hostname of syslog message producer

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- program name, which is appslogs
- log entry

Note: The log entries do not share a common format, as the number and type of fields in an entry is function-specific.

The following is a syslog record entry example:

```
Nov  9 11:10:28 nsp-1a3 appslogs: {app-specific_log_entry}
```

The fields in the example record have the following values:

- timestamp—Nov 9 11:10:28
- hostname of syslog entry producer—nsp-1a3
- program name—appslogs
- log entry—*function-specific_log_entry*, which is a comma-separated list of colon-separated attribute-value pairs that contain the log-entry message and other information, for example:

  `"attribute1":"value","attribute2":"value","attribute3":"value"`

14.6.3 NFM-P server syslog record format

Each NFM-P server log entry has the following fields:

- timestamp
- hostname of syslog message producer
- program name, which is nfmpserverlogs
- server log entry

The following is an example of a syslog record that contains an NFM-P server log entry:

```
Nov 7 05:40:15 nfmp-dc_1 nfmpserverlogs:{EMS_server_log_entry}
```

The fields in the example record have the following values:

- timestamp—Nov 7 05:40:15
- hostname of syslog entry producer—nfmp-dc_1
- program name—nfmpserverlogs
- server log entry—*EMS_server_log_entry*, which is a comma-separated list of colon-separated attribute-value pairs that contain the log-entry message and other information, for example:

  `"attribute1":"value","attribute2":"value","attribute3":"value"`

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part IV: NSP disaster recovery

Overview

Purpose

This part of the guide describes the redundancy functions employed by DR NSP clusters, and by integrated or ancillary NSP components deployed outside NSP clusters.

Contents

Chapter 15, Disaster recovery for NSP clusters	449
Chapter 16, Disaster recovery for NSP components	459

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

15 Disaster recovery for NSP clusters

15.1 What are the NSP cluster DR functions?

15.1.1 Description

The NSP disaster recovery (DR) function involves redundant NSP clusters in a warm standby configuration for fault tolerance in the event of a cluster failure. The following procedures describe how to control and manage NSP DR.

DR functions

The following NSP DR functions swap the primary and standby NSP cluster roles:

- failover—automatic DR role change initiated by the standby NSP cluster when a primary cluster failure is suspected
- switchover—manual DR operation that switches the NSP cluster roles

15.1.2 Failovers and switchovers

NSP DR failovers and switchovers are controlled by the ASM and role manager services, which run as the nspos-asm-app and nsp-role-manager pods in each DR NSP cluster. The standby role manager checks the connectivity to the role manager in the primary NSP cluster every ten seconds with an application-level HTTPS check.

When communication between two clusters is disrupted for more than two minutes, where the role manager cannot confirm connectivity between the standby and active cluster, the standby cluster assumes the primary role. When the fault is resolved, the NSP automatically returns to normal operation with functional active and standby clusters, where the active cluster has been up the longest.

In addition, the ASM service monitors essential primary pods and services such as the following:

- ZooKeeper
- Kafka
- PostgreSQL
- nspos-tomcat
- nsp-tomcat
- Keycloak
- prometheus-server

If any base service in a DR deployment is unavailable for more than three minutes, or two instances of a service in an HA+DR deployment are unavailable for more than three minutes:

- a failover occurs; consequently, the peer NSP cluster assumes the primary role
- an alarm is raised against the service or containing pod to indicate that the service or pod is down

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: Such an alarm may not be generated because of a base service disruption, depending on the circumstances.

- a major ActivitySwitch alarm is raised against the former active site, which is now the standby site

15.3 “How do I identify the NSP cluster DR roles?” (p. 452) describes how to display which role—primary or standby—is assigned to each NSP cluster. To restore the initial cluster roles after a failover, you perform a manual switchover, as described in 15.4 “How do I perform an NSP DR switchover from the NSP UI?” (p. 453).

Note: After a failover or switchover, NSP functions restart processes that were interrupted. If downstream functions are not up yet, the restarted processes may fail. For example, if a network configuration deployment was auditing at the time of a failover, the audit will restart when Infrastructure Configuration Management is up. If Network Intents is not back up yet when the audit is restarted, the audit will fail. The process can be restarted manually when the NSP has stabilized.

Disabling and enabling failovers

NSP DR failovers are enabled by default in a DR NSP deployment. If required, you can disable failovers to prevent disruption during a period of maintenance activity, as described in 15.6 “How do I disable NSP DR failovers?” (p. 455)

15.5 “How do I display the NSP DR failover setting?” (p. 454) describes how to identify whether failovers are enabled.

Note: The failover setting persists through an NSP software upgrade.

Note: For maximum fault tolerance, failovers must be disabled only during a maintenance period, and re-enabled after the maintenance period, as described in 15.7 “How do I enable NSP DR failovers?” (p. 456).

15.1.3 DR Cluster switchovers on the NSP UI

The System Health dashboard displays the primary and standby NSP cluster roles in a DR deployment. It can show both sites even when connectivity issues prevent communication between the two sites.

From the dashboard, the NSP administrator can manually trigger a switchover between the primary and standby clusters without logging into a cluster node and swap the cluster roles.

15.1.4 Standby cluster alarms

The NSP raises the following alarms for a standby NSP cluster:

- PodDownAlarm
- DiskSpaceBelowThresholdAlarm
- NodeMemoryBelowThresholdAlarm
- ServerMemoryBelowThresholdAlarm
- BaseServiceDownAlarm (InstanceDown)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- ClusterNodeDownAlarm

Before you take action to respond to an alarm, you must clearly identify the system raising the alarm and the node or pod at fault.

For better visibility in the standby cluster, the Source Type field of an alarm indicates the Site ID, Site Name, or Alarmed Object Name.

- The Site ID has this format: dc-name:node-name
- The Site Name has this format: dc-name:node-name
- The Alarmed Object Name has this format: dc-name:node-name:pod-name

Where dc-name is the DR data center name

When the pod is pending, the node-name is N/A.

For example, the Source Type field of a ServerMemoryBelowThreshold alarm, the operator has to view the Site ID, Site Name, or Alarmed Object Name field to identify which pod is at fault.

- If the Site ID is DR1:node1, node1 in the DR1 data center is at fault.
- If the Site Name is DR1:dr1-node1, dr1-node1 in the DR1 data center is at fault.
- If the Alarmed Object Name is DR1:dr1-node1:nspos-app1-tomcat-jmx-svc, the nspos-app1-tomcat-jmx-svc pod on dr1-node1 in the DR1 data center is at fault.

15.2 Pathway: prepare for an NSP DR switchover

15.2.1 Description

Before you perform an NSP DR switchover, you must ensure that the conditions are in place for a successful reversal of the primary and standby NSP cluster roles.

The following sequence of high-level actions describes how to ensure that the primary and standby NSP clusters are in the correct state for a successful DR switchover.

15.2.2 Stages

1

Use the System Health dashboard to verify that there are no outstanding Critical or Major alarms against any NSP cluster and to check the node status.

2

On the primary cluster, verify that each pod listed in the following table is in the state shown.

On the standby cluster, ensure that all pads are running, including the pods in the following table.

Pod	Primary cluster	Standby cluster
nspos-zookeeper	Running	Running
nspos-postgresql [1]	Running	Running

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Pod	Primary cluster	Standby cluster
nspos-tomcat	Running	Running
nspos-prometheus	Running	Running
nspos-kafka	Running	n/a
nsp-tomcat	Running	Running
nspos-keycloak	Running	Running
nspos-oauth2-proxy	Running	Running
nspos-asm-app	Running	Running
nsp-role-mgr	Running	Running
nsp-file-service-app [2]	Running	Running

Notes:

1. Restarts during switchover to change role and functions
2. If present; pod not required in all deployment types

3

Perform 15.3 “How do I identify the NSP cluster DR roles?” (p. 452) on each cluster.

4

Perform 13.1 “How do I check NSP database synchronization?” (p. 405) to ensure that the primary and standby databases are 100% synchronized.

15.3 How do I identify the NSP cluster DR roles?

15.3.1 Purpose

Perform this procedure to identify which NSP clusters in a DR deployment have the primary and standby roles.

If the System Health dashboard is not accessible, see “To identify the NSP cluster DR roles” in the *NSP Troubleshooting Guide* for the CLI procedure.

15.3.2 Steps

Identify cluster DR roles from the NSP UI

1

As an NSP administrator, choose **System Health** from the NSP main menu on the NSP UI.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Go to the Kubernetes cluster status.

3

View the status of the active and standby clusters.

The current cluster role is in the *Dc Role* field.

END OF STEPS

15.4 How do I perform an NSP DR switchover from the NSP UI?

15.4.1 Purpose



CAUTION

Service disruption

Performing this procedure causes a temporary loss of network visibility, which may be service-affecting.

You must perform the procedure only with the assistance of technical support during a scheduled maintenance period.

Perform this procedure on the System Health dashboard to initiate a switchover in a DR deployment.

If the System Health dashboard is not accessible, see “To perform an NSP DR switchover in a CLI” in the *NSP Troubleshooting Guide* for the CLI procedure.

15.4.2 Steps

1

As an NSP administrator, choose **System Health** from the NSP main menu on the NSP UI.

2

Go to the active (primary) cluster:

3

Hover over the ⋮ **More** icon on the right side of the cluster and **Make standby**.

A warning dialog box about service disruption appears. See the following caution.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

CAUTION

Service Disruption

Performing this procedure causes a temporary loss of network visibility, which may be service-affecting.

Ensure that no operations are performed on the DR clusters during the switchover.

Note: Triggering a switchover forces the roles on both clusters to change regardless of the Auto-failover setting.
Check the Auto-failover setting in 15.5 “How do I display the NSP DR failover setting?” (p. 453)

Click **Proceed** to continue with the switchover.

During the switchover, the DR cluster status disappears and then the remaining dashlets on the System Health dashboard disappear.

You are redirected to the standby cluster.

5

Log in as the NSP administrator.

6

Choose **System Health** from the NSP main menu on the NSP UI.

You can see the status of the DR cluster after the switchover.

END OF STEPS

15.5 How do I display the NSP DR failover setting?

15.5.1 Purpose

Perform this procedure to identify whether failovers are enabled in a DR NSP deployment.

Note: You require root user privileges on the NSP cluster host in each data center.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

15.5.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host in either data center.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm/ {print
$1;exit}')  -it $(kubectl get pods -A| awk '/nspos-asm/ {print
$2;exit}') -c nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl
autoFailoverStatus ↵
```

The following is displayed:

```
Current Auto-failover is: value
```

where *value* is one of the following:

- True—failovers are enabled
- False—failovers are disabled

4

Close the console window.

END OF STEPS

15.6 How do I disable NSP DR failovers?

15.6.1 Purpose

Perform this procedure to disable the failover function in a DR NSP deployment.

Note: Disabling the NSP failover function is intended to be a temporary measure for system maintenance purposes only. It is strongly recommended that you re-enable failovers after any maintenance that requires failovers to be disabled.

Note: You require root user privileges on the NSP cluster host in a data center.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

15.6.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host in either data center.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm/ {print
$1;exit}')  -it $(kubectl get pods -A| awk '/nspos-asm/ {print
$2;exit}') -c nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl
disableAutoFailover ↵
```

The following is displayed:

```
Auto-failover successfully disabled
```

4

Perform 15.3 “How do I identify the NSP cluster DR roles?” (p. 452) to verify that the cluster roles are unchanged.

5

Close the open console windows.

END OF STEPS

15.7 How do I enable NSP DR failovers?

15.7.1 Purpose

Perform this procedure to enable the failover function in a DR NSP deployment.

Note: You require root user privileges on the NSP cluster host in each data center.

Note: A leading # character in a command line represents the root user prompt, and is not to be included in a typed command.

15.7.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host in either data center.

2

Open a console window.

3

Enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm/ {print
$1;exit}')  -it $(kubectl get pods -A| awk '/nspos-asm/ {print
$2;exit}') -c nspos-asm-app -- /opt/nsp/os/asm/bin/asmctl
enableAutoFailover ↵
```

The following is displayed:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Auto-failover successfully enabled
```

4

Perform 15.3 “How do I identify the NSP cluster DR roles?” (p. 452) to verify that the cluster roles are unchanged.

5

Close the open console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16 Disaster recovery for NSP components

16.1 What are the NSP component DR functions?

16.1.1 Overview

In a DR NSP deployment, ancillary or optional NSP components deployed outside the NSP clusters have different redundancy mechanisms. In some scenarios, administrative action may be required to restore redundant operation, or to realign the component roles in a data center after a failed component is restored to operation:

- NSP auxiliary database clusters—see 16.2.1 “Auxiliary database geographic redundancy” (p. 459)
- NFM-P—see 16.4 “What is classic management redundancy?” (p. 463)

16.2 What is auxiliary database redundancy?

16.2.1 Auxiliary database geographic redundancy

A geographically redundant, or geo-redundant, auxiliary database has one cluster of one, or three or more, auxiliary database stations in each NSP data center. The cluster that is designated the primary cluster processes transactions; the other cluster acts as a warm standby in the event of a primary cluster failure.

The primary cluster replicates the incremental database content changes on the standby cluster every 30 minutes. Because the primary database updates are not immediately replicated, some data loss may occur under failure or switchover conditions.

Auxilary database failovers

An auxiliary database failover is non-revertive; a manual switchover is required to restore the former cluster roles when the failed cluster returns to service; see 16.3 “How do I perform an auxiliary database switchover?” (p. 460) for information.

NSP Analytics uses the primary auxiliary database as a data source. In the event of a primary auxiliary database cluster failure and resulting failover to the standby cluster, no operator intervention is required to restore Analytics functions, which automatically begin to use the new primary auxiliary database cluster.

16.2.2 Auxiliary database cluster switchover on the NSP UI

The System Health dashboard displays the primary and standby cluster roles for an auxiliary database cluster.

The dashboard also displays information such as the auxiliary database backup status, next backup, last backup, and copy cluster status.

From the dashboard, the NSP administrator can manually trigger a switchover between the primary and standby auxiliary database clusters.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

After the first copy-cluster operation, the NSP administrator can trigger a switchover. When copy-cluster is copying, is unavailable, or fails, the **Make active** button for the standby cluster disappears on the dashboard.

If the auxiliary database backup is running, the switchover operation must not be performed until the backup is complete.

If a cluster node is down, the copy-cluster operation cannot be performed.

If a standby cluster node is down, the **Make active** button for the standby cluster disappears on the dashboard.

16.3 How do I perform an auxiliary database switchover?

16.3.1 Purpose



CAUTION

Data Loss

Performing an auxiliary database switchover may result in an data-collection interruption of up to 30 minutes.

Ensure that you perform the switchover directly after the completion of the most recent copy-cluster operation, as described in the procedure.

Perform this procedure to switch the primary and standby roles of a geo-redundant auxiliary database.

The switchover operation can be performed only when all standby nodes are up and the copy-cluster operation is successful; the copy cluster status is not copy failed, copying, or unavailable.

If the auxiliary database backup is running, the switchover operation must not be performed until the backup is complete.

16.3.2 Steps

Perform an auxiliary database switchover from the NSP UI

1

As an NSP administrator, choose **System Health** from the NSP main menu on the NSP UI.

2

Go to the Auxiliary Database Clusters section.

3

Review the copy cluster status information.

If a copy-cluster operation is in progress, wait until the operation completes.

If not, identify the most recent copy-cluster completion time.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: To minimize data loss during a switchover, you must perform the switchover as soon as possible after the completion of a copy-cluster operation.

4

Click the **Show nodes** button in the standby cluster section.

Review the status information to confirm all standby cluster nodes statuses are ready.

5

Hover over the ⋮ **More** icon on the right side of the cluster and **Make active**.

A warning dialog box appears.

6

Click **Proceed** to continue with the switchover.

Wait about 10 minutes.

The roles reverse; the former standby cluster assumes the primary role.

END OF STEPS

16.3.3 Steps

Perform an auxiliary database switchover in a CLI

1

Log in to a station that has access to the NSP system.

2

Open a console window.

3

A copy-cluster operation is invoked every 30 minutes to replicate the recent data from the primary to the standby auxiliary database cluster.

You must identify the status of the most recent copy-cluster operation in order to determine when to perform the switchover.

Issue the following RESTCONF API call:

Note: In order to issue a RESTCONF API call, you require a token; see the My First NSP API Client tutorial on the Network Developer Portal for information.

`GET https://address/restconf/data/auxdb:auxdb-agent`

where *address* is the NSP advertised address

The auxiliary database cluster status is displayed; a copy-cluster operation is in progress when the status is RUNNING, and is complete when the status is SUCCESS.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Review the status information; if a copy-cluster operation is in progress, return to Step 3; otherwise, identify the most recent copy-cluster completion time.

Note: To minimize data loss during a switchover, you must perform the switchover as soon as possible after the completion of a copy-cluster operation.

5

Issue the following RESTCONF API call:

GET https://*address*/restconf/data/auxdb:clusters

where *address* is the NSP advertised address

The auxiliary database cluster node status is displayed; a standby cluster node is reachable when the node status is READY, and is unreachable when the node status is DOWN.

6

Review the status information to confirm all standby cluster nodes statuses are ready.

7

Plan to perform the auxiliary database switchover as soon as possible after the completion of a copy-cluster operation.

8

At the time planned in Step 7, perform the switchover by issuing the following RESTCONF API call:

POST https://*address*/restconf/data/auxdb:clusters/cluster=*cluster_ID*/activate

where

address is the NSP advertised address

cluster_ID is the target-cluster value in the Step 3 command output

The request body is required to send the call to switch over now:

```
{
    "auxdb:input" : {
    }
}
```

9

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16.4 What is classic management redundancy?

16.4.1 Redundancy functions

NFM-P system redundancy is initially configured during system deployment. You use the NFM-P GUI, or scripts on a main server station, to perform the following redundancy functions:

- Check the main server and database redundancy status.
- Manually switch the primary and standby main server roles.
- Enable or disable automatic database realignment.
- Reinstantiate the former primary database as the standby database.

You can configure the following redundancy parameters to specify how an NFM-P system manages a loss of connection to the managed NEs; contact technical support for more information:

- the number of elapsed seconds that constitute a loss of connectivity
- how often a main server refreshes the list of managed NEs
- the minimum number of NEs that must respond to a connectivity check

16.5 What are the NFM-P system redundancy models?

16.5.1 Overview



CAUTION

Service Disruption

It is recommended that you deploy the primary server and database in the same geographical location and LAN.

This results in increased NFM-P system performance and fault tolerance.

A redundant NFM-P system provides greater fault tolerance by ensuring that there is no single point of software failure in the NFM-P management network. A redundant system consists of the following components:

- primary and standby main servers
- primary and standby main databases

The current state of a component defines the primary or standby role of the component. The primary main server actively manages the network and the primary database is open in read/write mode. When a standby component detects a primary component failure, it automatically changes roles from standby to primary. You can also change the role of a component using the NFM-P client GUI or a CLI script.

The NFM-P supports collocated and distributed system redundancy. A collocated system requires two stations that each host a main server and database. A distributed system requires four stations that each host a main server or database. Each main server and database is logically independent, regardless of the deployment type.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The primary and standby main servers communicate with the redundant databases and periodically verify server redundancy. If the standby server fails to reach the primary server within 60s, the standby server becomes a primary server. See 16.7 “How do I respond to NFM-P redundancy failures?” (p. 474) for information about various NFM-P redundancy failure scenarios.

A main database uses the Oracle DataGuard function to maintain redundancy. During a redundant NFM-P installation or upgrade, the Oracle DataGuard synchronization level is set to real-time apply, which ensures that the primary and standby databases are synchronized.

Figure 16-1 Collocated redundant NFM-P deployment

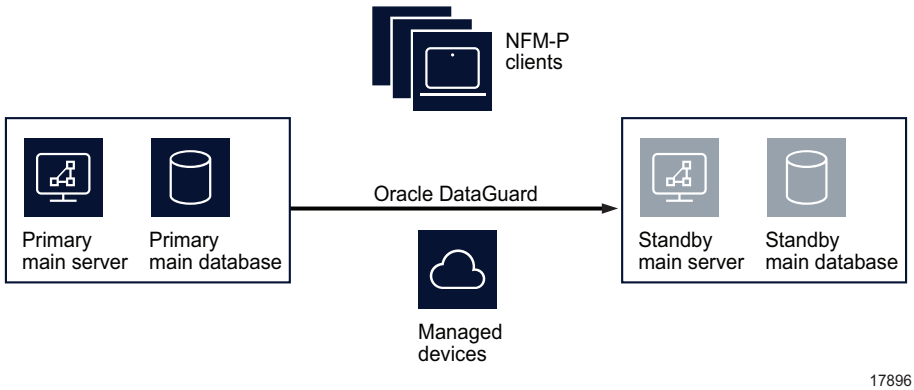
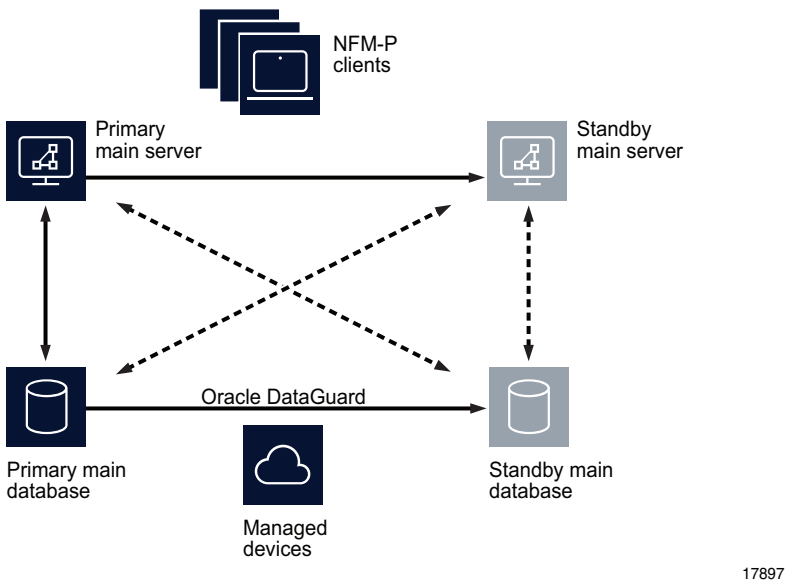


Figure 16-2 Distributed redundant NFM-P deployment



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

A main server role change is called a server activity switch. An automatic database role change is called a failover; a manual database role change is called a switchover.

A typical redundant NFM-P system has a primary server and database in a geographically separate facility from the standby server and database facility. To ensure that the primary components are in the same LAN after an activity switch or failover, you can configure automatic database realignment during a main server installation or upgrade. See 16.6.6 “Automatic database realignment” (p. 471) for more information.

The NFM-P GUI, browser, and XML API clients must always communicate with the current primary main server. After a server activity switch or switchover:

- The GUI clients automatically connect to the new primary main server, which is the former standby.
- The XML API and browser clients do not automatically connect to the new primary main server; you must redirect each browser and XML API client to the new primary main server.

The following general conditions apply to NFM-P system redundancy:

- The main servers and databases must each be redundant. For example, you cannot have redundant servers and a standalone database.
- The network that contains a redundant NFM-P system must meet the latency and bandwidth requirements described in the *NSP NFM-P Planning Guide*.

  Note: To provide hardware fault tolerance in addition to software redundancy, it is recommended that you use redundant physical links between the primary and standby servers and databases to ensure there is no single point of network or hardware failure.
- The server and database stations require the same OS version and patch level.
- The server stations require identical disk layouts and partitioning.
- The database stations require identical disk layouts and partitioning.
- Only the nsp user on a main server station can perform a server activity switch.
- The following users can perform a database switchover:
  - nsp user on a main server station
  - NFM-P GUI user with update or execute permissions on the following classes:
    db.DatabaseManager.switchover
    db.DatabaseManager.reinstantiateStandby
  - NFM-P GUI user with the admin scope of command role

16.5.2 Auxiliary server redundancy

NFM-P auxiliary servers are optional servers that extend the network management processing engine by distributing server functions among multiple stations. An NFM-P main server controls task scheduling and sends task requests to auxiliary servers. Each auxiliary server is installed on a separate station, and responds to processing requests only from the current primary main server in a redundant system.

When an auxiliary server cannot connect to the primary main server or database, it re-initializes and continues trying to connect until it succeeds or, in the case of a database failover, until the main server directs it to the peer database.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

After startup, an auxiliary server waits for initialization information from a main server. An auxiliary server restarts if it does not receive all required initialization information within five minutes.

Note: NFM-P system performance may degrade when a main server loses contact with a number of auxiliary servers that exceeds the number of Preferred auxiliary servers.

When an auxiliary server fails to respond to a primary main server, the main server tries repeatedly to establish communication before it generates an alarm. The alarm clears when the communication is re-established.

Auxiliary server types

The auxiliary servers in an NFM-P system are specified in each main server configuration, which includes the address of each auxiliary server in the system, and the auxiliary server type, which is one of the following:

- Preferred—processes requests under normal conditions
- Reserved—processes requests when a Preferred auxiliary server is unavailable
- Remote Standby—unused by the main server; processes requests only from the peer main server, and only when the peer main server is operating as the primary main server

If a Preferred auxiliary server is unresponsive, the main server directs the requests to another Preferred auxiliary server, if available, or to a Reserved auxiliary server. When the unresponsive Preferred auxiliary server returns to service, the main server reverts to the Preferred auxiliary server and stops sending requests to any Reserved auxiliary server that had assumed the Preferred workload.

An auxiliary server that is specified as a Remote Standby auxiliary server is a Preferred or Reserved auxiliary server of the peer main server. The Remote Standby designation of an auxiliary server in a main server configuration ensures that the main server does not use the auxiliary server under any circumstances. Such a configuration may be required when the network latency between the primary and standby main servers is high, for example, when the NFM-P system is geographically dispersed.

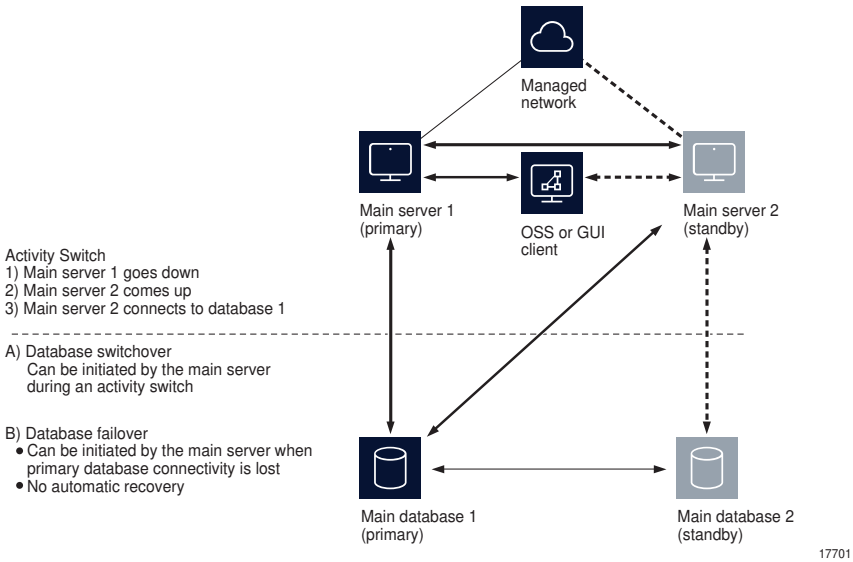
Alternatively, if all main and auxiliary servers are in the same physical facility and the network latency between components is not a concern, no Remote Standby designation is required, and you can apply the Preferred and Reserved designations based on your requirements. For example, you may choose to configure a Preferred auxiliary server of one main server as the Reserved auxiliary server of the peer main server, and a Reserved auxiliary server as the Preferred of the peer main server.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16.6 What are the NFM-P redundancy functions?

16.6.1 Overview

Figure 16-3 NFM-P redundancy role-change functions



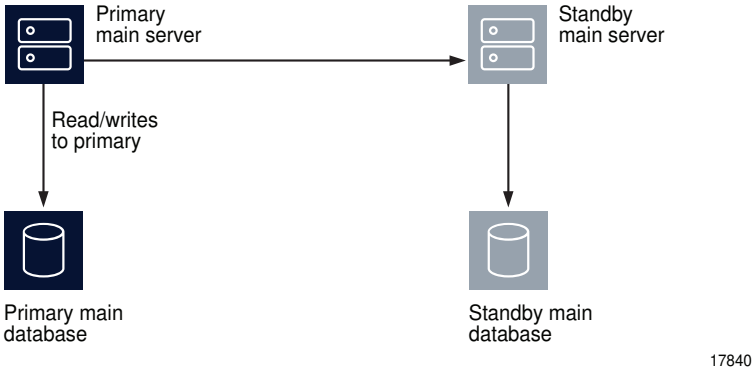
16.6.2 Server activity switches

The standby server initiates an automatic server activity switch when it cannot communicate with the primary server. An NFM-P administrator can perform a manual server activity switch, which is typically a planned server maintenance or test operation.

Note: For security reasons, you cannot use an NFM-P GUI or XML API client to perform a server activity switch.

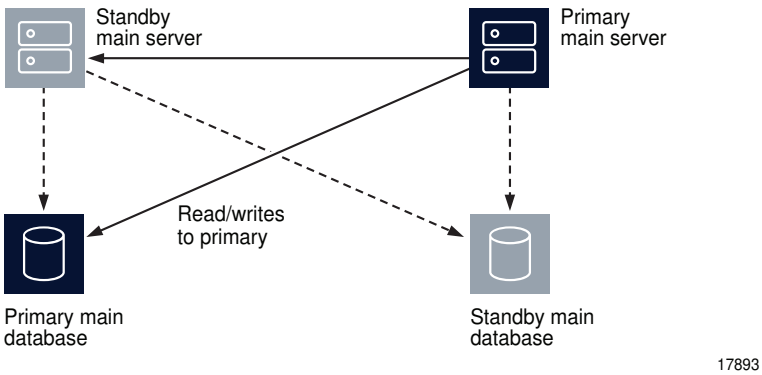
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 16-4 Server and database roles before server activity switch



The NFM-P raises alarms when a server activity switch is initiated. During the activity switch, the main servers do not process SNMP traps, attempt to synchronize NEs, or collect statistics. Auxiliary servers process outstanding requests, but do not communicate with a main server.

Figure 16-5 Server and database roles after server activity switch



After a server activity switch:

- If automatic database realignment is enabled, the new primary main server performs a database switchover.
- All browser and XML API clients require redirection to the new primary main server.
- The new primary server establishes communication and synchronizes information with the auxiliary servers.
- The auxiliary servers exchange information with the new primary server; no auxiliary servers exchange information with the former primary server.
- The Preferred or Reserved state of each auxiliary server changes, depending on the configuration of the new primary server.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- The new primary server attempts to redeploy the client requests that the former primary server did not complete before the activity switch.

16.6.3 Database switchovers

An NFM-P administrator directs a main server to initiate a database switchover.

Figure 16-6 Server and database roles before database switchover

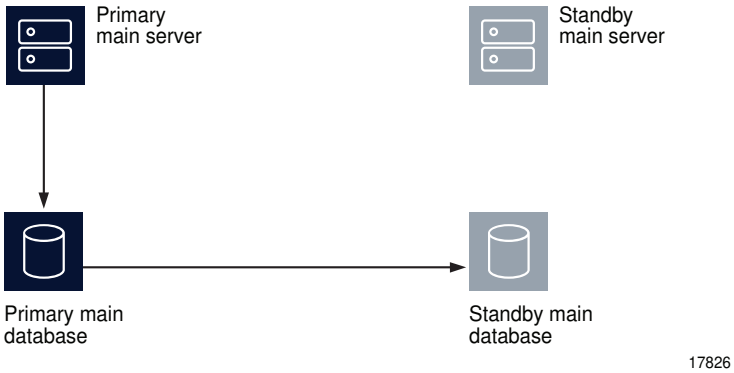
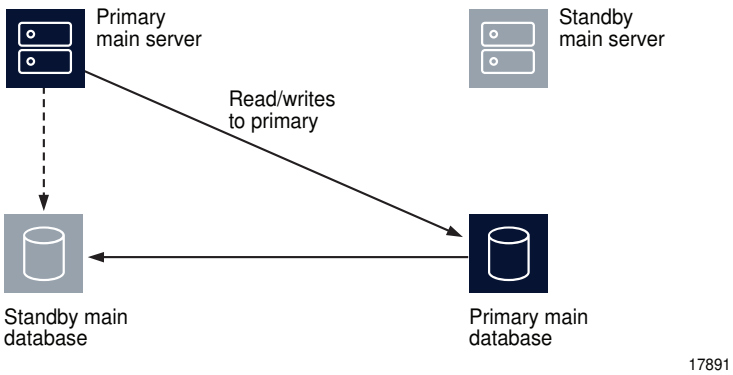


Figure 16-7 Server and database roles after database switchover



The following occurs after a successful database switchover:

- The primary server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary server directs each auxiliary server to use the new primary database.

When a database switchover fails, the primary and standby database roles do not change. No automatic database realignment occurs as a result of a switchover.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16.6.4 Database failovers

The main database failover function is enabled by default. A failover occurs when a main server cannot communicate with the primary database, but can communicate with the standby database and the managed NEs. When this happens, the main server directs the standby database to become the primary database.

A database failover occurs only if the following conditions are true.

- The standby database is configured, operational, and reachable.
- The main server can communicate with the managed NEs.

Figure 16-8 Server and database roles before database failover

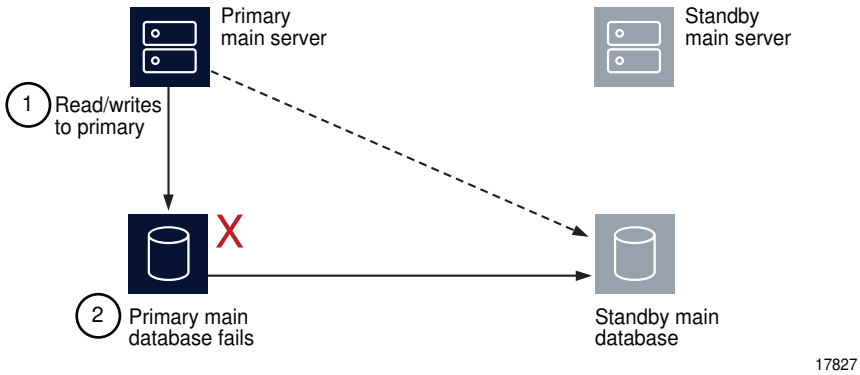
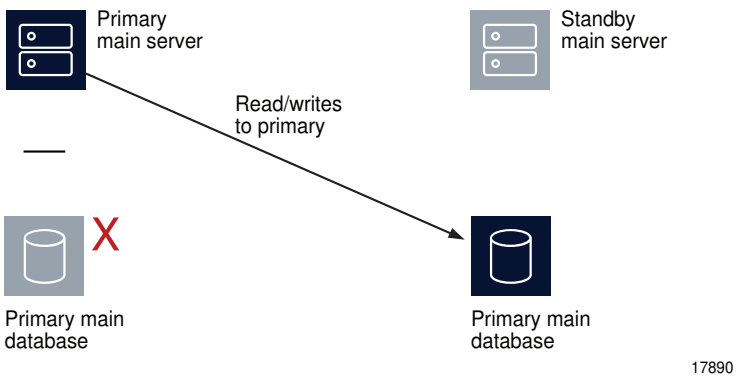


Figure 16-9 Server and database roles after database failover



When a database failover fails, the primary server tries again to communicate with the primary database. If the primary database remains unavailable, the primary server tries again to initiate a failover.

Note: During a database failover, a network management outage occurs; the GUI clients can

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

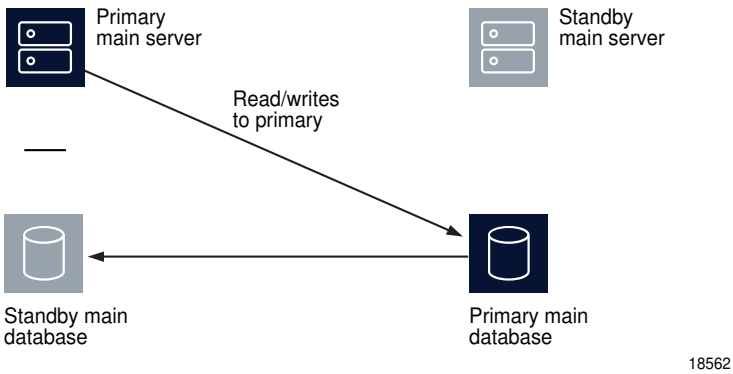
monitor the failover, but cannot perform configuration activities.

Note: After a successful failover, database redundancy is not available until the new primary database is reinstantiated as the standby database on the former primary database station. See 16.6.5 “Re-establishing database redundancy” (p. 470) for more information.

16.6.5 Re-establishing database redundancy

After a failover, the former primary database is no longer part of the redundant configuration. To re-establish database redundancy, you must reinstantiate the former primary database as the new standby database. You can do this only when the failed database station is restored to full operation and has a functional proxy port. See 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) and 22.21 “How do I reinstantiate the main database from a CLI?” (p. 756) for information about how to reinstantiate a database.

Figure 16-10 Server and database roles after database reinstantiation



Automatic database reinstantiation

You can configure the NFM-P to automatically reinstantiate the former primary database as the new standby database. Automatic database reinstantiation occurs only in the event of a database failover. When the function is enabled, the NFM-P attempts an automatic reinstantiation every 60 minutes by default. You can enable automatic database reinstantiation during a main server installation or upgrade. See the *NSP Installation and Upgrade Guide* for information about enabling and configuring automatic database reinstantiation.

16.6.6 Automatic database realignment

In a redundant NFM-P system that is geographically dispersed, the primary main server and database may be in separate LANs or WANs after an activity switch or failover. The network latency that this introduces can affect NFM-P system performance. Automatic database realignment is an optional mechanism that attempts to ensure that each main server uses the local database.

The database with which a main server tries to align itself is called the preferred database of the main server. An operator enables automatic database realignment and specifies the preferred database during NFM-P server installation, or during server configuration after installation.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: For automatic database alignment to work, you must enable it and specify a preferred database on each main server in a redundant NFM-P system.

When a primary server starts, it verifies that the primary database is the preferred database. If the primary database is not the preferred database, the server performs a database switchover to reverse the primary and standby database roles. If the switchover is successful, the main servers and databases in the NFM-P system are aligned. If the switchover fails, each database reverts to the former role, and the main server generates an alarm about the failed switchover.

When you perform a database switchover and automatic database realignment is enabled, the primary server does not attempt database realignment. A switchover is a manual operation that is considered to be a purposeful act.

Performing a server activity switch when automatic database realignment is enabled triggers a database switchover.

16.6.7 Redundancy function summary

Table 16-1 Redundancy functions, main server

Function	Notes
Automatic server activity switch An automatic activity switch occurs when the primary server cannot communicate with the standby server, and involves the following sequence of events. • The standby server cannot communicate with the primary server within 60 seconds, or the primary server cannot communicate with the managed network. • The standby server performs an activity switch to become the new primary server. The activity switch occurs only if the standby server can communicate with the managed network. • If automatic database realignment is enabled, the new primary server attempts a database switchover. • The new primary server connects to the primary database and manages the network. • The new primary server and the auxiliary servers synchronize the outstanding request information.	During an activity switch, each browser client and XML API client loses connectivity with the primary main server. During an activity switch, a main server does not process SNMP traps from the network, and no NE re-synchronizations occur. The auxiliary servers continue to process outstanding requests, and synchronize the request information with the new primary server after the activity switch. When the communication failure is resolved, you must re-open each browser client, and redirect each XML API client to the new primary main server.
Manual server activity switch A manual activity switch is typically performed for maintenance or testing during a scheduled period of low activity, and involves the following sequence of events. • An NFM-P administrator initiates the activity switch on the primary server. • The standby server performs an activity switch to become the new primary server. • The new primary server connects to the primary database and manages the network. • The new primary server and the auxiliary servers synchronize the request information. • If automatic database realignment is enabled, the new primary server attempts a database switchover.	

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 16-2 Redundancy functions, main database

Function	Notes
Database switchover A database switchover is a manual operation that reverses the primary and standby database roles, for example, for primary database maintenance, or to realign database roles with database stations after a server activity switch. A switchover can occur only when the primary and standby databases are functioning correctly and can communicate with each other. A database switchover involves the following sequence of events. • An NFM-P administrator initiates the switchover on a primary or standby server. • The main server asks each auxiliary server to release all database connections. The switchover fails if all database connections are not released within 15 minutes. • The main server directs the standby database to become the primary database. • The main server fully synchronizes information with the new primary database. See 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) for information about performing a database switchover.	No automatic database realignment occurs after a database switchover.
Database failover A database failover is an automatic operation that changes the standby database into a primary database when the original primary database is unreachable, for example, because of a power disruption on the primary database station. A database failover involves the following sequence of events. • No main server can communicate with the primary database within a period that is 2 min by default. • The primary main server directs the standby database to become the primary database. • If automatic database realignment is enabled and the primary server and database are not aligned, the primary server performs an activity switch. • The primary server directs each auxiliary server to connect to the new primary database. • The main server restarts after a failover.	When the primary server detects a communication failure with the primary or standby database: • The GUI clients are informed that the database is not reachable. • A network management outage begins; the GUI clients can monitor the failover, but cannot perform configuration activities. After the cause of the communication failure is resolved, the GUI clients are notified that the database is reachable, and the network management outage ends. After the failover, you must reinstantiate the former primary database as the new standby database to restore database redundancy. **Note:** If automatic database reinstantiation is enabled, the NFM-P automatically attempts to reinstantiate the former primary database.
Re-establishing database redundancy Re-establishing database redundancy after a database failure requires database reinstantiation to replicate the current primary database as the standby database. After a failover, the former primary database is not available for redundancy until an operator or the automatic database reinstantiation function reinstantiates it as the new standby database. See 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) and 22.21 “How do I reinstantiate the main database from a CLI?” (p. 756) for information about re-establishing database redundancy after a failover.	The following conditions must be met before you can re-establish database redundancy. • The failover completes successfully. • The station that contains the former primary database is operational. • The former primary database proxy port is configured and in service.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16.7 How do I respond to NFM-P redundancy failures?

16.7.1 Overview

The following describe the NFM-P actions in response to various types of redundancy failures.

- **Primary server loses contact with primary database**

  If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs.

  If automatic database realignment is enabled, the new primary server performs a database switchover.

- **Primary server loses contact with managed NEs**

  If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch.

  If automatic database realignment is enabled, the new primary server performs a database switchover.

- **Primary server loses contact with primary database and managed NEs**

  If the standby server can communicate with the primary database and the managed NEs, the primary server performs a server activity switch. No database failover occurs.

  If automatic database realignment is enabled, the new primary server performs a database switchover.

- **Primary server loses contact with primary database, managed NEs, and standby server**

  The standby server activates to become the new primary server, and if automatic database realignment is enabled, initiates a database switchover.

- **Both servers lose contact with primary database**

  The primary server initiates a database failover, and if automatic database realignment is enabled, also initiates a server activity switch.

- **Both servers lose contact, primary server and database can communicate**

  The primary server and database remain the primary server and database. The NFM-P raises an alarm about the server communication failure.

- **Both servers lose contact with managed NEs**

  If the primary and standby servers can each communicate with the preferred database, no server activity switch or database failover occurs. The NFM-P raises a reachability alarm against each NE in the network.

- **Both servers lose contact with primary database and managed NEs**

  If the primary and standby servers can communicate with each other, no server activity switch or database failover occurs. However, the NFM-P system is unavailable; manual intervention such as a database failover is required.

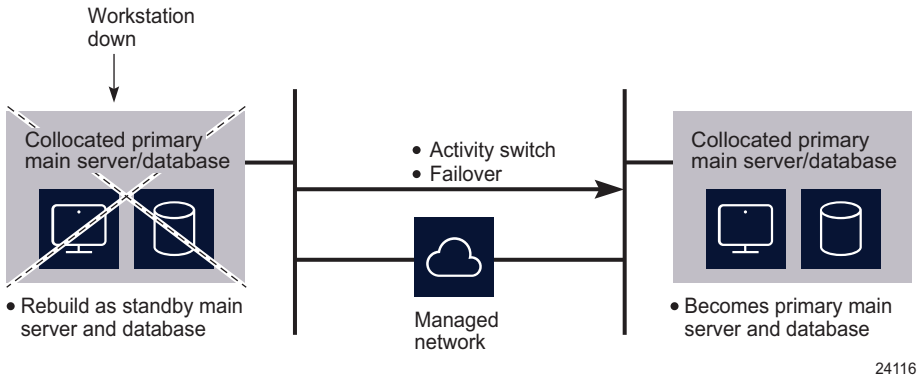
- **Both servers fail, primary database isolated, standby database operational**

  When both servers return to operation, the servers cannot connect to the primary database. Because the state of the standby database is unknown, no database failover occurs; manual intervention such as a database switchover is required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16.7.2 Collocated system, primary station unreachable

Figure 16-11 Primary server and database station down, collocated system

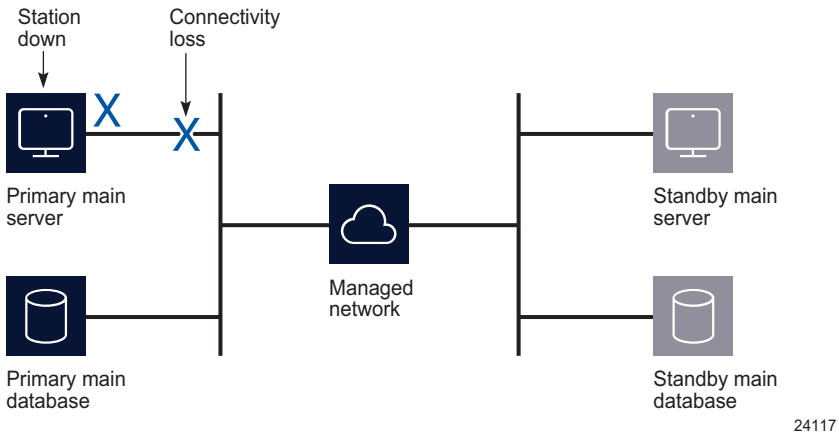


The following occur when the primary station becomes unresponsive:

- The standby server and database become the primary server and database.
- Redundancy is restored when the former primary station returns to service as the standby station.

16.7.3 Distributed system, primary server unreachable

Figure 16-12 Primary server unreachable, distributed system



The following occur when the primary station becomes unresponsive:

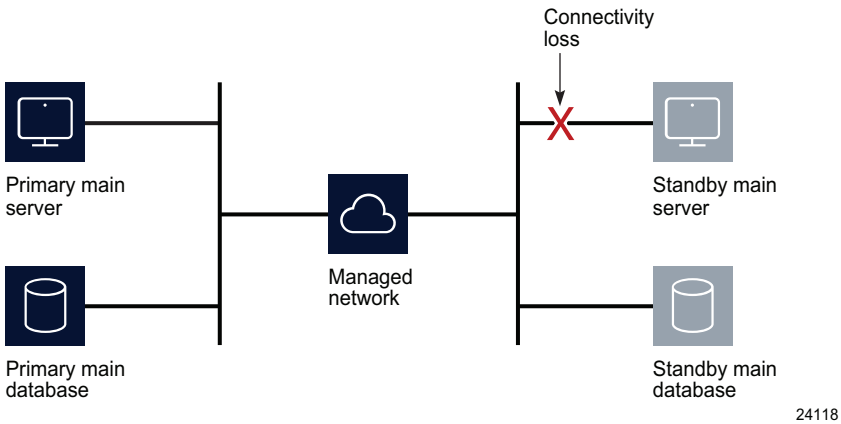
- The standby server detects the connectivity loss and becomes the primary server.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- The new primary main server raises alarms about the unavailability of the former standby, and about the activity switch.
- If automatic database realignment is enabled, the new primary server initiates a database switchover.
- When connectivity is restored, the former primary server assumes the standby server role.

16.7.4 Distributed system, standby server unreachable

Figure 16-13 Standby server unreachable, distributed system



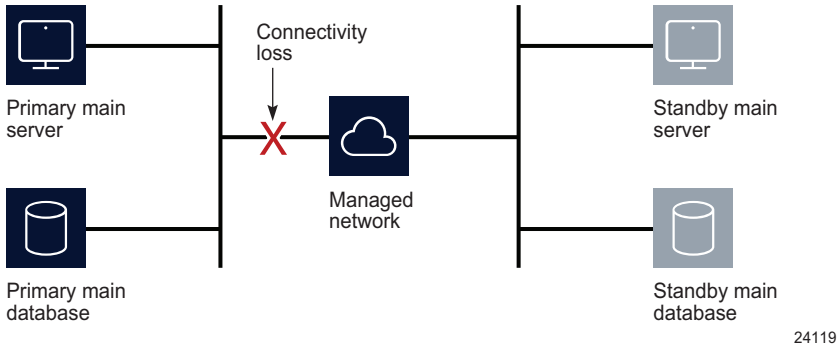
The following occur when the standby station becomes unresponsive:

- The standby server interprets the primary server unresponsiveness as a primary server failure, so attempts to assume the primary server role.
- The primary server generates an alarm to indicate that the standby server is down.
- When the reachability is restored, the standby server resumes the standby role and the alarm clears.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16.7.5 Distributed system, managed network unreachable by primary side

Figure 16-14 Network failure on primary side, distributed system



The following occur after the connectivity loss is detected:

- The initial primary server continues to operate as a primary server.
- The initial primary server generates an alarm about the standby server unavailability, and a reachability alarm against each NE in the network.
- Each GUI client displays the standby server status as Down.
- The standby server becomes a primary server.

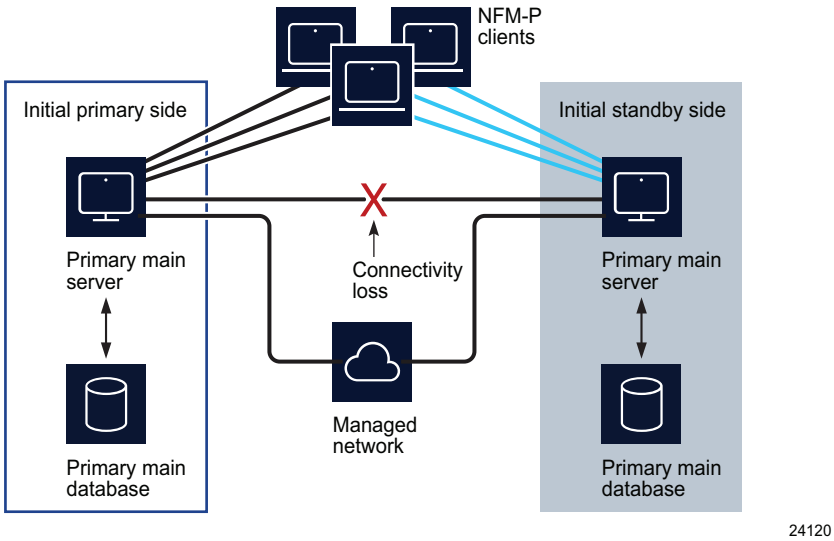
Note: You can eliminate a single point of hardware or network failure by using redundant interfaces and redundant physical network paths. See the *NSP NFM-P Planning Guide* for more information.

16.7.6 Split complex

A split complex is a scenario in which both servers in a collocated or distributed system lose contact, but each server can communicate with the preferred database, as shown in the following figure.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Figure 16-15 Split complex, collocated or distributed system



The following occur after the connectivity loss is detected:

- The initial primary server and database roles do not change; the initial primary server continues to manage the network. The client sessions are not interrupted.
- The primary server raises an alarm about the communication failure.
- The standby server and database switch roles to become a second primary server and database.
- New clients connect to the initial primary server; however, if a client explicitly tries to connect to the second primary server, a session is established.
- When the servers regain contact:
  - If the network disruption also isolates one server from the managed NEs, the other server and database remain the primary.
  - Otherwise, the server that has currently held the primary role for longer remains the primary, and the other server and database assume the standby role,

16.8 Pathway: manage NFM-P redundancy

16.8.1 Stages

1

As required, perform server activity switches and database switchovers.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

a.

For main servers:

1. View the status of the primary and secondary servers to verify the redundancy status is Up; see 16.9 “How do I view the NFM-P system redundancy status?” (p. 479) .
2. If required, verify the redundancy status of the NFM-P auxiliary server; see 16.10 “How do I view the NFM-P auxiliary server status?” (p. 482) .
3. Perform a manual activity switch to reverse the primary and standby roles; see 16.11 “How do I perform a server activity switch?” (p. 484).
4. Validate the updated redundancy status; see 16.9 “How do I view the NFM-P system redundancy status?” (p. 479).

b.

For main databases:

1. View the redundancy status of the primary and secondary database to verify the redundancy status is Up; see 16.9 “How do I view the NFM-P system redundancy status?” (p. 479).
2. As required, specify the behavior of how database switchovers are executed; see 16.12 “How do I configure main database switchover behavior?” (p. 485).
3. As required, perform a database switchover; see 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) or 16.14 “How do I perform a main database switchover using a CLI script?” (p. 487).
4. As required, enable or disable automatic database realignment; see 16.15 “How do I enable or disable automatic database realignment?” (p. 488).
5. Validate the updated redundancy status; see 16.9 “How do I view the NFM-P system redundancy status?” (p. 479).

2

After a main database failover, re-establish redundancy between the standby and primary databases; see 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) and 22.21 “How do I reinstantiate the main database from a CLI?” (p. 756).

16.9 How do I view the NFM-P system redundancy status?

16.9.1 Steps

1

View the Standby Server, Primary DB and Standby DB status indicators in the NFM-P client GUI task bar. Each indicator must display Up.

2

Choose Administration→System Information. The System Information form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

View the general redundancy information:

- Domain Name—the NFM-P domain name specified at installation
- Redundancy Enabled—selected if redundancy is enabled
- Realignment Enabled—selected if automatic database realignment is enabled; displayed only if the NFM-P system is redundant
- Auto Standby Re-instantiation Enabled
- Realignment Status—Aligned or Not Aligned

4

View the following information in the Primary Server panel:

- Host Name—the host name of the primary or standalone main server
- Preferred DB—the preferred database of the main server
- Status—Unknown, Down, or Up

5

View the following information in the Primary Database Server panel:

- Instance Name—the name of the primary database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the primary database
- Host Name—the host name of the primary or standalone main database

6

If the NFM-P system is redundant, view the following information in the Standby Server panel:

- Host Name—the host name of the standby main server
- Status—Unknown, Down, or Up

7

If the NFM-P system is redundant, view the following information in the Standby Database Server panel:

- Instance Name—the name of the standby database instance, also called a SID
- IP Address—the IP address that each main or auxiliary server uses to reach the standby database
- Host Name—the host name of the standby database

8

Click Properties to display additional information about the primary or standby main server. The Main Server (Edit) properties form opens.

9

View the following general main-server information:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Host Name—the host name of the primary main server
- Server Type—Main
- Resource Managed—selected if the main server is included in NFM-P resource management

10

View the following information in the Client Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the NFM-P GUI, browser, and XML API clients through a NAT router
- Public IP Address—the IP address that the NFM-P GUI, browser, and XML API clients use to reach the main server through a NAT router

Note: The Private IP Address and Public IP Address display 0.0.0.0 when the NFM-P clients and the main server use host names, rather than IP addresses, for communication. The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and clients.

11

View the following information in the Redundant Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the standby main server through a NAT router
- Public IP Address—the IP address that the standby main server uses to reach the primary main server through a NAT router
- Peer Public IP Address—the IP address that the standby main server uses to reach the main server

Note: The Private IP Address and Public IP Address display the same IP address when NAT is not used between the primary and standby main servers.

12

View the following information in the Redundancy Database State panel:

- Switchover State—whether switchover in progress, and operational state
- Last Attempted Switchover Time—time of previous switchover attempt
- Failover State—whether failover in progress, and operational state
- Last Attempted Failover Time—time of previous failover attempt
- Standby Re-instantiation State—whether reinstantiation is in progress, and operational state
- Last Attempted Standby Re-instantiation Time—time of previous standby reinstantiation attempt
- Number of Archive Logs To be Applied—number of archive logs that remain to be applied on standby database
- Estimated Time to Apply Archive Logs (seconds)—system time estimate for archive-log synchronization with standby database

13

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

View the following information in the Auxiliary Server Communication panel:

- Private IP Address—the IP address that the main server uses as the source address for communication with the auxiliary servers through a NAT router
- Public IP Address—the IP address that the auxiliary servers use to reach the primary main server

Note: The Private IP Address and Public IP Address display the same IP address when NAT is not used between the main server and the auxiliary servers.

14

View the following information in the Main Server Communication panel:

- Server Public IP Address—the IP address that the auxiliary server uses to communicate with the main server

15

Close the Main Server properties form.

16

Click Database to view detailed database information, if required.

17

Click on the Faults tab to view alarm information, if required.

18

Close the form.

END OF STEPS

16.10 How do I view the NFM-P auxiliary server status?

16.10.1 Steps

1

Choose Administration→System Information. The System Information form opens.

2

Click on the Auxiliary Servers tab.

3

Review the list of auxiliary servers.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Select an auxiliary server in the list and click Properties. The properties form for the auxiliary server opens.

5

Review the auxiliary server information, which includes the following:

- Host Name—the host name of the auxiliary server
- Port Number—identifies the port that the auxiliary server uses to communicate with each main server and database
- Auxiliary Server Type—Reserved or Preferred
- Server Status—Unknown, Down, Up or Unused
- Resource Managed—selected if the auxiliary server is included in NFM-P resource management
- Public IP address—the IP address that the main servers use to reach the auxiliary server

6

Perform one of the following:

a. View the following main server information for a redundant system:
   - Server 1 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server
   - Server 2 Public IP address—the IP address that the auxiliary server uses to communicate with the primary or standby main server

b. View the following main server information for a standalone system:
   - Server Public IP address—the IP address that the auxiliary server uses to communicate with the main server

7

Click on the Auxiliary Services tab.

8

Review the list of auxiliary services.

9

Review the information for each auxiliary service, which includes the following:

- Service Name—the type of service, for example, statistics collection
- Selected—indicates whether this auxiliary server is currently used by a main server to process requests
- IP Address—the IPv4 address that the managed NEs use to reach the auxiliary server
- IPv6 Address—the IPv6 address that the managed Wavence NEs use to reach the auxiliary server
- Host Name—the host name of this auxiliary server

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Auxiliary Server Type—Reserved or Preferred

10

Close the Auxiliary Services form.

11

Click on the Faults tab to view alarm information, if required.

12

Close the form.

END OF STEPS

16.11 How do I perform a server activity switch?

16.11.1 Purpose

Perform this procedure to reverse the primary and standby roles of the main servers in a redundant system. Consider the following before you perform a server activity switch.

- A server activity switch stops and starts the primary main server. Server redundancy is unavailable until the main server is fully initialized as the new standby main server.
- During a server activity switch:
  - The NFM-P raises an alarm about the activity switch; the alarm is not self-clearing.
  - A main server does not process SNMP traps, attempt to synchronize NEs, or collect statistics.
  - All GUI, browser, and clients lose connectivity to the NFM-P.
  - Auxiliary servers process outstanding requests, but do not communicate with a main server.
- After a server activity switch:
  - The new primary main server deploys outstanding configuration changes to NEs, establishes communication with the auxiliary servers, and synchronizes information with the auxiliary servers.
  - The GUI clients automatically connect to the new primary main server.
  - XML API and browser clients must be redirected to the new primary main server.

16.11.2 Steps

1

Log in to the primary main server station as the nsp user.

2

Open a console window.

3

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash force_restart ↵
```

The server activity switch begins. The primary main server restarts as the standby main server, and the standby main server restarts as the primary.

4

When the activity switch is complete, close the console window.

5

Reconnect each browser client to the NFM-P.

1. Close the browser window.
2. Open the browser window.

Note: After an activity switch, depending on the state of the former primary main server station, the NFM-P automatically redirects sign-in requests to the new primary main server. If the redirection fails to occur, you must open the sign-in page using the address of the new primary main server.

6

Redirect each XML API client to the new primary main server.

7

Manually clear the activity switch alarms, as required.

END OF STEPS

16.12 How do I configure main database switchover behavior?

16.12.1 Purpose

Perform this procedure on a redundant system to specify how database switchovers are executed. A database switchover occurs immediately upon request unless a database query is in progress, in which case the NFM-P does the following:

- if session interruption is enabled, waits a specified period before forcing the switchover
- if session interruption is disabled, the switchover does not occur and the Switchover State is Failed

16.12.2 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager (Edit) form opens.

2

Configure the required parameters:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- DB Session wait time (minutes)
- Interrupt Read sessions after time out
- Interrupt Write sessions after time out

3

Save your changes and close the form.

END OF STEPS

16.13 How do I perform a main database switchover using the NFM-P client GUI?

16.13.1 Purpose

Perform this procedure to use the NFM-P client GUI to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.



CAUTION

Service Disruption

The execution of a database switchover depends on how the database switchover behavior is configured.

It is recommended that you review 16.12 “How do I configure main database switchover behavior?” (p. 485) before you attempt to perform this procedure to verify the current database switchover configuration.

16.13.2 Steps

1

Log in to the client GUI as a user with the admin scope of command role.

2

Choose Administration→System Information from the NFM-P main menu. The System Information form opens.

3

Click Switchover and respond to the dialog box prompt.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The Switchover option is disabled when the correct switchover conditions are not in place, for example, when a switchover or failover is in progress.

4

Click Yes. The NFM-P server performs the database switchover.

5

Close the form.

END OF STEPS

16.14 How do I perform a main database switchover using a CLI script?

16.14.1 Purpose

Perform this procedure to use a CLI script to switch the primary and standby database roles. Before you perform the procedure, ensure that you understand the following implications of a switchover.

- The primary and standby database roles are reversed.
- The primary main server connects to the new primary database.
- Archive logging begins on the new primary database.
- The primary main server directs each auxiliary server to connect to the new primary database.

CAUTION

Service Disruption

The execution of a database switchover depends on how the database switchover behavior is configured.

It is recommended that you review 16.12 "How do I configure main database switchover behavior?" (p. 485) before you attempt to perform this procedure to verify the current database switchover configuration.

16.14.2 Steps

1

Log in to the primary main server station as the nsp user.

2

Open a console window.

3

Enter the following at the CLI prompt:

```
bash$ /opt/nsp/nfmp/server/nms/bin/switchoverdb.bash -u username -p password ↵
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

where *username* and *password* are the login credentials of an NFM-P user with the required privilege level and scope of command

The script displays the following confirmation message:

```
The standby database will become the new primary database, and the old
primary will become the new standby. Do you want to proceed? (YES/no)
:
```

4

Enter the following to initiate the switchover:

YES ↵

The NFM-P server initiates a database switchover. Progress is indicated by a rolling display of dots in the console window. The database switchover is complete when the CLI prompt reappears.

5

Close the console window when the database switchover is complete.

END OF STEPS

16.15 How do I enable or disable automatic database realignment?

CAUTION

Service Disruption

This procedure requires a primary main server restart, which is service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.

Note: This procedure applies only to redundant systems.

16.15.1 Steps

1

Perform Step 4 to Step 14 on the standby main server station.

2

Perform Step 4 to Step 14 on the primary main server station.

Note: When you stop the primary main server, a switchover to the standby main server occurs.

3

Go to Step 15.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Log in to the main server as the nsp user.

5

Stop the main server.

1. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

2. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

6

Enter the following to switch to the root user:

```
bash$ su - ↲
```

7

Enter the following:

```
# samconfig -m main ↲
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

8

Perform one of the following:

a. Enable database alignment; perform the following steps.

1. Enter the following:

   ```
   <main> configure redundancy database alignment ↲
   ```

   Database alignment is enabled, and the prompt changes to `<main configure redundancy database>`.

2. Enter the following:

   ```
   <main configure redundancy database> prefer-instance instance ↲
   ```

   where *instance* is the database instance with which the main server is to align, typically the database instance on the same side of the management LAN

b. Disable database alignment; perform the following steps.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Enter the following:

   `<main>` **`configure redundancy database no alignment`** ↵

   Database alignment is disabled, and the prompt changes to `<main configure redundancy database>`.

9

Enter the following:

`<main configure redundancy database>` **`exit`** ↵

The prompt changes to `<main>`.

10

Enter the following:

`<main>` **`apply`** ↵

The configuration change is applied.

11

Enter the following:

`<main>` **`exit`** ↵

The samconfig utility closes.

12

Enter the following to switch back to the nsp user:

`#` **`exit`** ↵

13

Start the main server.

1. Enter the following:

   `bash$` **`cd /opt/nsp/nfmp/server/nms/bin`** ↵

2. Enter the following:

   `bash$` **`./nmsserver.bash start`** ↵

3. Enter the following:

   `bash$` **`./nmsserver.bash appserver_status`** ↵

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

14

Log out of the main server station.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

15

If required, perform 16.11 “How do I perform a server activity switch?” (p. 484) to perform a server activity switch to revert the primary and standby main servers to their initial roles.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Part V: NSP component administration

Overview

Purpose

This part of the *NSP System Administrator Guide* provides information about managing NSP system elements that are deployed outside the NSP cluster or treated as discrete functions that require occasional administration or configuration.

Contents

Chapter 17, MDM administration	495
Chapter 18, Artifact administration	515
Chapter 19, Telemetry administration	519
Chapter 20, NSP auxiliary database administration	521
Chapter 21, Classic management administration	589
Chapter 22, Classic management database administration	707

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17 MDM administration

17.1 What is MDM administration?

17.1.1 Description

In general, MDM administration consists of:

- adaptor artifact management: MDM adaptors are a type of NSP artifact. Adaptor artifacts for NSP releases prior to 25.8 cannot be managed from the Artifacts views in the NSP GUI.
  - For more information about artifacts, see “Artifact Management” in the *NSP Network Automation Guide*.
  - For information about the adaptors required for a specific NE, see the artifact guide for the NE.
- TLS and mTLS configuration
- management of YANG model definitions and NE model definitions
- device mapping files for telemetry and resync

The procedures in this chapter describe operations performed on NSP host servers to support model-driven mediation.

Note: The procedures in this chapter include the following RHEL CLI prompts in command lines to denote the active user. They are not to be included in typed commands:

- # —root user
- bash$ —nsp user

17.2 What should I know about adaptor artifact management?

17.2.1 Adaptor artifacts

MDM adaptors are a type of NSP artifact used for management of model-driven devices. While many NSP artifacts, including adaptor artifact bundles, can be installed using the Artifacts view in the NSP GUI, adaptor suites for NSP releases prior to 25.8 must be installed using a script; see 17.3 “How do I install artifacts that are not supported in the Artifacts view?” (p. 496). See the artifact documentation provided with the adaptor artifacts for information about which installation method is required.

It is not necessary to uninstall adaptor artifacts before installing a new iteration of the adaptation artifact bundle or adaptor suite. When the new iteration is installed the adaptors are upgraded, but obsolete artifacts and artifact bundles remain in the NSP.

If a constraint applies to a specific adaptation artifact bundle, uninstalling the old version may be recommended. Any constraints that apply are described in the artifact documentation.

You do not need to restart the NSP after installing an adaptation artifact bundle.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17.2.2 Uninstalling artifacts

If you need to uninstall an artifact that was installed using a script, you must use a script for the uninstallation; see 17.8 “How do I uninstall MDM adaptor suites?” (p. 508).

17.3 How do I install artifacts that are not supported in the Artifacts view?

17.3.1 Purpose

Perform this procedure to install or upgrade artifacts that are not supported in the Artifacts view, such as adaptor suites from releases prior to 25.8.

While many NSP artifacts can be installed using the Artifacts view in the NSP GUI, some must be installed by script using this procedure. See the artifact documentation provided with the adaptor artifacts for information about which installation method is required.

Nokia recommends installing all adaptors in any adaptor suite.

17.3.2 Before you begin

If you require custom or reference adaptors for your network, contact Nokia.

The following must be true before you attempt to perform the procedure:

- The NSP system includes MDM and is operational.
- The NSP clusters, MDM servers, mdm-tomcat service, and file service are initialized and operational.

Note: In this procedure, *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

17.3.3 Steps

CAUTION

Deployment Failure

You may need to uninstall one or more existing adaptors before you install a new adaptor, or the adaptor installation fails.

Before you install an adaptor, ensure that you read the adaptor artifact documentation to determine whether any existing adaptors conflict with the new adaptor and must be removed before the new adaptor installation. If no conflicts are mentioned in the artifact documentation, you can proceed with the installation without uninstalling any artifacts.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1

Obtain the artifacts and associated documentation from the Nokia NSP software delivery site, in the NSP/<release>/Adaptors folder.

2

Check the artifact documentation to see if any adaptors need to be removed before proceeding with the installation.

See 17.8 “How do I uninstall MDM adaptor suites?” (p. 508) to uninstall an adaptor suite if needed, then proceed to the next step.

3

Log in as the root or NSP admin user on the NSP deployer VM in the standalone or primary NSP cluster.

Note: In a DR deployment, you perform the installation or upgrade only on the primary NSP cluster, which then replicates the adaptor configuration to the standby cluster.

4

Transfer the adaptor suite zip file to an empty temporary directory.

5

Open a console window.

6

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin ↵
```

7

Enter the following to verify that the RESTCONF token for the NSP cluster is valid:

```
# ./adaptor-suite.bash --list ↵
```

Enter the NSP admin user credentials when prompted.

Messages like the following are displayed if the token is valid.

```
Using log file: log_file
INFO: timestamp -> Listing MDM adaptors suites ...
INFO: timestamp -> Token requested...
INFO: timestamp -> Token acquired
INFO: timestamp -> Listing adaptor suites...
Installed adaptor suites:
list_of_adaptors
INFO: timestamp -> Done.
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Enter the following:

Note: Multiple files and wildcards are supported. For example, sros* specifies all adaptor suites whose filenames begin with sros.

```
# ./adaptor-suite.bash --install filespec_1 filespec_2 . . .
filespec_n ↵
```

where

filespec_1 to *filespec_n* are one or more adaptor zip file specifications; each must include the absolute file path

Enter the NSP admin user credentials when prompted.

9

Enter the credentials.

The artifacts are transferred to each MDM instance.

Note: It may take 30 minutes or more for all artifacts to load.

10

If the NSP system is a DR deployment, verify that the primary and standby file-service-app pods are communicating.

1. Log in as the root or NSP admin user on the NSP cluster host in the standby NSP cluster.
2. Enter the following:

   ```
   # kubectl exec -n  $(kubectl get pods -A | awk
   '/nsp-file-service-app/ {print $1;exit}') -it
   nsp-file-service-app-0 -- ls
   /opt/nsp/containers/nspvolume/fileservice/nokia/nsp/mdm/features/suite/
   ↵
   ```

   Messages like the following are displayed, and the zip files are listed.

   ```
   Defaulting container name to nsp-file-service-app
   Use 'kubectl describe pod/nsp-file-service-app-0 -n default' to see
   all of the containers in this pod.
   ```

   If the zip files are listed, the primary and standby pods are communicating; the artifacts are installed on the standby cluster upon DR activation of the standby cluster.

11

Close the open console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17.4 How do I enable mTLS on the NSP mediation interface?

17.4.1 Purpose

Perform this procedure to enable mutual TLS authentication (or mTLS) on the network mediation interface of an NSP cluster.

The NSP client private key file, client public certificate file, and CA public certificate file must be configured before starting this procedure; see 7.13 “How do I add an NSP Kubernetes secret?” (p. 130)

Note: You must perform this procedure in each NSP cluster.

17.4.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

4

Configure the following parameters in the **nsp**—**modules**—**mdm** section of the file:

```
mtls:
  enabled: true
  mtlsKeyAlgorithm: "RSA"
```

5

Save and close the file.

6

Open a console window.

7

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

8

Enter the following to update the mTLS Kubernetes server secret:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ./nspdeployerctl secret -s mediation-mtls-key -n
"nsp-psa-privileged" -f tls.key=mtlsKey -f tls.crt=mtlsClientCert -f
ca.crt=mtlsCACert update
# ./nspdeployerctl secret -s mediation-mtls-key -n
"nsp-psa-restricted" -f tls.key=mtlsKey -f tls.crt=mtlsClientCert -f
ca.crt=mtlsCACert update
```

where

mtlsKey is the full path of the client private key file

mtlsClientCert is the full path of the client public certificate file

mtlsCACert is the full path of the CA public certificate file

Messages like the following are displayed as the server secret is updated:

```
secret/mediation-mtls-key patched
The following files may contain sensitive information. They are no
longer required by NSP and may be removed.
  mtlsKey
  mtlsClientCert
  mtlsCACert
```

9

Enter the following to put the configuration change into effect:

Note: The command causes a restart of each MDM pod in the cluster, but is not service-affecting.

```
# ./nspdeployerctl install --config --deploy ↵
```

mTLS is enabled on the cluster mediation interface.

END OF STEPS

17.5 How do I enable TLS and mTLS for telemetry and gNMI on_change support?

17.5.1 Purpose

To enable TLS communication between MDM and managed NEs, you must deploy a signed TLS certificate to each MDM-managed device that supports gRPC TLS, and import the CA certificates that allow MDM to validate that NE certificate. While it is possible to have more than one CA certificate added to each MDM truststore, to maintain network security it is preferable to limit the number of CA certificates to the minimum required.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

You can also enable mutual TLS authentication (mTLS) on the network mediation interface of the NSP clusters.

The following steps describe how to secure the following NSP communication with NEs by importing a TLS certificate:

- telemetry
- gNMI on_change notifications

CA certificates and certificate chains for gRPC TLS

In one-way TLS between NSP and the NE, the NE acts as the TLS server and MDM acts as the TLS client. MDM must trust the certificate chain presented by the NE: the truststore must contain every certificate required to build a certification path from the NE leaf certificate to a trusted anchor (PKIX validation).

If the NE leaf certificate is issued by an intermediate CA, importing only the root CA into the MDM truststore is often insufficient. Import the intermediate CA certificate (or certificates) as well as the root. You can concatenate intermediate and root PEM files into a single PEM file for placement under *tls/telemetry*, or place separate PEM files in that directory and import each certificate into the MDM truststore using a distinct *keytool* alias.

Before you import certificates into MDM, you can verify the chain against the NE certificate with OpenSSL; for example:

```
# openssl verify -CAfile root_CA.pem -untrusted intermediate_CA.pem
node.pem ↵
```

where *root_CA*.pem is the trust anchor, *intermediate_CA*.pem is the issuing intermediate (add another *-untrusted* option for each additional intermediate), and *node*.pem is the NE TLS certificate.

When you run *keytool -importcert* on a PEM file, only the first certificate in the file is typically imported. If a PEM file contains multiple certificates, split the file or import each certificate from a separate PEM file using a separate alias.

Some deployments have required both a combined chain PEM file and the root CA PEM file to remain in *tls/telemetry* for *nspdeployerctl install --config --deploy* to process telemetry TLS material as expected. If certificate deployment or gRPC TLS fails after you add only a chain file, add the root CA PEM in the same directory and retry the deploy step, or contact Nokia technical support for your NSP release.

You must perform the procedure on each NSP cluster in a DR deployment.

The TLS certificates for gRPC mediation are separate from the certificates used for internal NSP component communication and NSP client communication.

release-ID in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17.5.2 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Transfer the TLS certificate file, either to the following directory, or to another directory that you document for later steps:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tls/telemetry

You will require this path later in this procedure.

Note: You must not modify or delete any existing file in the directory.

4

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml

5

In the telemetry—gnmi—tls section of the file, configure the caCertPath parameter with the path you used in Step 3.

6

Save and close the file.

7

Enter the following command to put the certificate change into effect in the local TLS truststore for each MDM server:

```
# ./nspdeployerctl install --config --deploy.
```

The command restarts each MDM pod in the cluster.

8

Enter the following to update the mTLS Kubernetes server secret on the mediation interface:

```
# ./nspdeployerctl secret -s mediation-mtls-key -n
"nsp-psa-privileged" -f tls.key=mtlsKey -f tls.crt=mtlsClientCert -f
ca.crt=mtlsCACert update
```

```
# ./nspdeployerctl secret -s mediation-mtls-key -n
"nsp-psa-restricted" -f tls.key=mtlsKey -f tls.crt=mtlsClientCert -f
ca.crt=mtlsCACert update
```

where

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

mtlsKey is the full path of the client private key file

mtlsClientCert is the full path of the client public certificate file

mtlsCACert is the full path of the CA public certificate file

Messages like the following are displayed as the server secret is updated:

```
secret/mediation-mtls-key patched
The following files may contain sensitive information. They are no
longer required by NSP and may be removed.
  mtlsKey
  mtlsClientCert
  mtlsCACert
```

9

When the redeployment is complete, close the console window.

END OF STEPS

17.6 How do I manage MDM model definitions?

17.6.1 Purpose

The following steps describe how to manage the YANG model definitions and NE model definitions in an NSP cluster.

Note: The yang-files.bash script prompts for NSP administrative user credentials. To suppress the prompt, you can include the credentials in the script command line; for example:

```
# ./yang-files.bash --list --user user --pass password ↵
```

where *user* and *password* are the NSP administrative user credentials

For simplicity, the credentials and prompt are not shown in the procedure steps.

Note: The NSP system must be fully operational when you perform the procedure.

Note: If you are adding model definitions:

- The new model-definition files must be in a directory accessible to the NSP deployer VM.
- If a zipped collection of files is being installed, all files in the collection must be of the same type.

Note: If you are adding an NE model, the required files are in a compressed archive file; contact Nokia for access to the file.

Note: *release-ID* in a file path has the following format:

R.r.p-rel.*version*

where

R.r.p is the NSP release, in the form *MAJOR.minor.patch*

version is a numeric value

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17.6.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer VM in the standalone or primary NSP cluster.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin ↵
```

Manage YANG models

4

To list the names of all installed module sets, enter the following:

```
# ./yang-files.bash --list ↵
```

The module sets are listed.

5

To list the names of the YANG models in a module set, enter the following:

```
# ./yang-files.bash --modulesetname module_set --list ↵
```

where *module_set* is the module set name

The YANG model names are listed in the following format:

```
model_name -> (namespace,revision)
```

6

To save all YANG models in a module set as files, enter the following:

```
# ./yang-files.bash --modulesetname module_set --save path ↵
```

where

module_set is the module set name

path is an existing directory on the local file system

The model files are created in the specified directory.

7

To save specific YANG models in a module set as files, enter the following:

```
# ./yang-files.bash --modulesetname module_set --model model_1 model_2
. . . model_n --save path ↵
```

where

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

module_set is the module set name

model_1 model_2 . . . model_n is a list of the YANG models to save

path is an existing directory on the local file system

The model files are created in the specified directory.

8

To add one or more YANG model definitions, enter the following:

Note: Because of the heavy processing load associated with importing model definitions, it is strongly recommended that you do not attempt to install all YANG files in a bundle at once.
If you need to install a large number of YANG files, the recommended method is to install only the immediately required files, in small batches, and install any additional YANG files later, as required.
If the following message is displayed after you try to install YANG files, you may need to install fewer files at a time; you can use the command option in the message to verify that the current operation installed all specified files:
`WARN: Timeout uploading yang files. Please verify with --list --modulesetname module_set`

```
# ./yang-files.bash --modulesetname module_set --add path ↵
```

where

module_set is the module set name

path is the path to a YANG definition file, or to a directory that contains definition files

9

To remove one or more YANG model definitions, enter the following:

```
# ./yang-files.bash --modulesetname module_set --remove definition_1 definition_2 . . . definition_n ↵
```

where

module_set is the module set name

definition_1 definition_2 . . . definition_n is a list of model definitions in the following format:

modelname,*namespace*,*revision*

Add NE model definitions

10

To add one or more NE model definitions, enter the following:

```
# ./ne-model.bash --install definition_file ↵
```

where *definition_file* is the path and name of an NE model zip file

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Close the open console windows.

END OF STEPS

17.7 How do I manage MDM device mappings?

17.7.1 Purpose

The following steps describe how to manage the device mappings for MDM in an NSP cluster. You can use this procedure in the unusual case when mapping files have been delivered outside an artifact bundle.

Note: The NSP system must be fully operational when you perform the procedure.

Note: In order to add device mappings:

- The new device-mapping files must be in a directory accessible to the NSP deployer VM.
- If a zipped collection of files is being installed, all files in the collection must be of the same type, for example, telemetry device mappings.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

17.7.2 Steps

1

Log in as the root or NSP admin user on the NSP deployer VM in the standalone or primary NSP cluster.

2

Open a console window.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin ↵
```

4

To list the current device mappings, which are in JSON format, enter the following:

Note: The --ne option applies only to resync mappings, and is optional.

Note: The --class option applies only to nfmp-resync mappings, and is optional.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: If the --ne and --class options are omitted, all mappings of the specified type are listed.

Note: The --save option saves the list to a file, and is valid only for telemetry mappings.

```
# ./json-files.bash --list --mapping mapping_type --ne device_def
--class class_path --save path --user user --pass password ↵
```

where

mapping_type is one of the following mapping types: telemetry, resync, or nfmp-resync

device_def is a device type definition, for example, SR-7750,21.10.R1

class_path is the NFM-P class path of the device type, in XPath format

path is an existing local directory in which to save the mapping list

user and *password* are the credentials of an NSP administrative user

5

To add one or more JSON mapping files, enter the following:

```
# ./json-files.bash --add path --user user --pass password ↵
```

where

path is the path to a JSON mapping file, or to a directory that contains mapping files

user and *password* are the credentials of an NSP administrative user

6

Enter the following to remove one or more device mappings:

Note: The --filename option is required only for telemetry mappings.

Note: The --ne option applies only to resync mappings, and is optional.

Note: The --class option applies only to nfmp-resync mappings, and is optional.

Note: If the --ne and --class options are omitted, all mappings of the specified type are removed.

```
# ./json-files.bash --remove --mapping mapping_type --filename
mapping_1 mapping_2 ...mapping_n --ne device_type --class class_path
--user user --pass password ↵
```

where

mapping_type is one of the following mapping types: telemetry, resync, or nfmp-resync

mapping_1 mapping_2 ...mapping_n is a list of telemetry mapping files to remove

device_type is a device type definition, for example, SR-7750,21.10.R1; a value has the following format: neType,neVersion—for example, SR-7750,21.10.R1

class_path is the NFM-P class path of the device type, in XPath format

user and *password* are the credentials of an NSP administrative user

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Close the console window.

END OF STEPS

17.8 How do I uninstall MDM adaptor suites?

17.8.1 Purpose

Perform this procedure to permanently remove one or more MDM adaptor suites from the NSP.

Note: In a DR deployment, you perform the adaptor-suite uninstallation in the primary data center; the NSP file-service-app subsequently synchronizes the primary and standby adaptor configurations.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

17.8.2 Steps

WARNING

Network Management Degradation

After you remove an MDM adaptor suite, you cannot re-install or reinstantiate the adaptor suite using a restart of any pod in the local NSP cluster, or a DR switchover. Consequently, network management may be severely compromised.

Before you attempt to remove an MDM adaptor suite, you must ensure that there are no dependencies on any adaptor in the adaptor suite.

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user in the standalone or primary data center.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin ↵
```

4

Enter the following to verify that the RESTCONF token for the NSP cluster is valid:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# ./adaptor-suite.bash --list ↵
```

Enter the NSP admin user credentials when prompted.

Messages like the following are displayed if the token is valid.

```
Using log file: log_file
INFO: timestamp -> Listing MDM adaptors suites ...
INFO: timestamp -> Token requested...
INFO: timestamp -> Token acquired
INFO: timestamp -> Listing adaptor suites...
Installed adaptor suites:
list_of_adaptor_suites
INFO: timestamp -> Done.
```

5

It is strongly recommended to list the adaptor suites and check for network management dependencies before any adaptor suite is removed.

To list the adaptor suites on the file system, enter the following:

Note: The --list-adaptors option queries the installed adaptors on the MDM server; by contrast, the --list option displays the adaptor suites in the PostgreSQL database. Consequently, until the next periodic NSP cluster data synchronization, an adaptor that you remove may be temporarily shown in the --list option output.

Note: To filter the command output for a specific vendor, pipe the output to grep; for example, the following lists only adaptor suites whose name includes ‘sros’:
adaptor-suite.bash --list | grep sros ↵

```
# ./adaptor-suite.bash --list ↵
```

Enter the NSP admin user credentials when prompted.

6

Enter the following to remove one or more adaptor suites:

```
# ./adaptor-suite.bash --remove zipfile_1 zipfile_2 . . . zipfile_n ↵
```

where *zipfile_1* to *zipfile_n* are adaptor-suite zip-file specifications; each must include the absolute path

Enter the NSP admin user credentials when prompted.

7

Enter the NSP admin user credentials.

The adaptors are removed from each running MDM instance.

Note: It may take 30 minutes or more for adaptors to be removed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

If the NSP system is at Release 22.3 or later, enter the following to display the adaptor suites that the --cleanup option in Step 10 removes:

Note: The --list-cleanup option displays the adaptor suites that are uninstalled from the MDM servers but still available in the PostgreSQL database and file-service-app pod.

```
# ./adaptor-suite.bash --list-cleanup ↵
```

Enter the NSP admin user credentials when prompted.

9

If the NSP system is a DR deployment, verify that the primary and standby file-service-app pods are communicating.

1. Log in as the root or NSP admin user on the NSP cluster host in the primary NSP cluster.
2. Enter the following:

   ```
   # kubectl exec -n  $(kubectl get pods -A | awk
   '/nsp-file-service-app/ {print $1;exit}') -it
   nsp-file-service-app-0 -- ls
   /opt/nsp/containers/nspvolume/fileservice/nokia/nsp/mdm/features/suite/↵
   ```

   Messages like the following are displayed, and the MDM adaptor zip files are listed.

   ```
   Defaulting container name to nsp-file-service-app

   Use 'kubectl describe pod/nsp-file-service-app-0 -n default' to see
   all of the containers in this pod.
   ```

3. Log in as the root or NSP admin user on the NSP cluster host in the standby NSP cluster.
4. Open a console window.
5. Enter the following:

   ```
   # kubectl exec -n  $(kubectl get pods -A | awk
   '/nsp-file-service-app/ {print $1;exit}') -it
   nsp-file-service-app-0 -- ls
   /opt/nsp/containers/nspvolume/fileservice/nokia/nsp/mdm/features/suite/↵
   ```

   Messages like the following are displayed, and the MDM adaptor zip files are listed.

   ```
   Defaulting container name to nsp-file-service-app

   Use 'kubectl describe pod/nsp-file-service-app-0 -n default' to see
   all of the containers in this pod.
   ```

6. Compare the lists of adaptor zip files on the primary and standby file-service-app pods.

   If the lists match, the file-service-app pods are communicating correctly.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10

WARNING

Network Management Degradation

In a DR NSP deployment, performing this step when the adaptors on the primary and standby clusters do not match may severely degrade network management and require a cluster redeployment.

Before you perform the step in a DR deployment, you must be certain that the list of installed adaptors on the standby MDM servers matches the list of installed adaptors on the primary MDM servers.

Enter the following to delete all references to all uninstalled adaptor suites from the PostgreSQL database and file-service-app:

```
# ./adaptor-suite.bash --cleanup ↵
```

Enter the NSP admin user credentials when prompted.

All references to the uninstalled adaptor suites are removed.

11

Close the console window.

END OF STEPS

17.9 How do I restart an MDM server?

17.9.1 Purpose

Perform the following steps to restart an MDM server in an NSP cluster.

17.9.2 Steps

1

Log in as the root or NSP admin user on the NSP cluster host.

2

Open a console window.

3

Enter the following to display the MDM server instances:

```
# kubectl get pods -A | grep mdm-server ↵
```

The MDM server instances and pod numbers are listed.

4

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# kubectl delete pod mdm-server-n -n $(kubectl get pods -A | awk
'/mdm-server/ {print $1;exit}') ↵
```

where *n* is the MDM server pod number

The MDM server restarts.

5

Repeat Step 4 to restart an additional MDM server, as required.

6

Close the console window.

END OF STEPS

17.10 How do I retrieve detailed information about MDM servers?

Note: The NSP system must be operational before these operations can be performed.

17.10.1 Steps

1

Open a terminal session to the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin/ ↵
```

4

Enter the following to show the MDM server roles, the number of NEs managed using MDM, and which MDM server is hosting which NE:

```
# ./server-load.bash --user username --pass password --detail ↵
```

where

username is the NSP username

password is the NSP password

5

The command output includes information such as the following:

```
{
    "mdmInstanceInfos": [
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
        {
            "name": mdm-server-0,
            "ipAddress": mdm-server-0.mdm-server-svc-headless.default.
svc.cluster.local,
            "grpcPort": 30000,
            "status": Up,
            "neCount": 0,
            "neIds": null,
            "active": False
            "groupIds": [1, 2],
        },
        {
            "name": mdm-server-1,
            "ipAddress": mdm-server-1.mdm-server-svc-headless.default.
svc.cluster.local,
            "grpcPort": 30000,
            "status": Up,
            "neCount": 2,
            "neIds": ["1.1.1.1", "1.1.1.2"],
            "active": True
            "groupId": 1,
        },
        {
            "name": mdm-server-2,
            "ipAddress": mdm-server-2.mdm-server-svc-headless.default.
svc.cluster.local,
            "grpcPort": 30000,
            "status": Up,
            "neCount": 2,
            "neIds": ["1.1.1.3", "1.1.1.4"],
            "active": True
            "groupId": 2,
        }
    ]
}
```


END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17.11 How do I rebalance NE load on MDM servers?

Note: The NSP system must be operational before these operations can be performed.

17.11.1 Steps

1

Open a terminal session on the NSP deployer VM.

2

Log in as the root or NSP admin user.

3

Enter the following:

cd /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tools/mdm/bin/↵

4

Enter the following to show the MDM server roles, the number of NEs managed using MDM, and which MDM server is hosting which NE:

./server-load.bash --user *username* --pass *password* --rebalance↵

where

username is the NSP username

password is the NSP password

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

18 Artifact administration

18.1 What is NSP artifact administration?

18.1.1 Artifacts

NSP administrators are responsible for obtaining, importing, and installing the Nokia-provided NSP artifacts that are required for model-driven management of various Nokia and multivendor devices. Pluggable NSP artifacts produced by Nokia are delivered on the software delivery site both with and between NSP releases.

See “What is an artifact?” in the *NSP Network Automation Guide* for overview information about artifacts, and the “Artifact management” chapter in the *NSP Network Automation Guide* for information about managing artifact bundles in the NSP UI.

18.1.2 Signatures

Signatures provide visibility of the authorship of an artifact bundle, and ability to easily verify that the bundle comes from a trusted source.

Artifact bundles created by Nokia are signed by Nokia and do not require NSP administrative action.

However, NSP administrators are responsible for managing the authenticity of artifact bundles created in-house.

The procedures in this chapter describe operations performed on NSP host servers to support signing customer-created artifact bundles.

Note: Installation of artifact bundles that are not signed by Nokia, including self-signed or unsigned artifact bundles, requires an NSP license that includes the NSP Developer feature pack.

Public/private key pairs

Signing artifact bundles requires the creation of a public/private key pair. To ensure authenticity of artifacts, artifact bundles are signed with a private key that must only be known to the original artifact bundle developer.

The corresponding public key is installed, along with the corresponding author name, in NSP. When a signed artifact bundle is installed, NSP looks up the corresponding public key registered for the author name and validates the artifact bundle signature. The private key must be stored in a safe place.

After the keys are generated, the public key and the bundle author name are saved to a secret YAML file, which is loaded into Kubernetes.

The secret file must be saved to all standby sites in a DR NSP deployment. If an NSP upgrade requires removal of Kubernetes resources such as secrets, the files will need to be loaded again after the upgrade is completed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Nokia recommends backing up all secret YAML files before performing an NSP upgrade.

18.2 How do I create a public/private key pair?

18.2.1 Purpose

Use this procedure to create a public/private key pair, save the public key to a secret YAML file, and load the secret file to Kubernetes.

This procedure uses the openssl tool, version 3.0.3 or later. The tool should be available by default in a Linux environment.

Author names containing potentially confusing keywords, such as “NSP”, or “N0k1a” are blocked. If a secret file is created with a blocked author name, the signature is invalid and the bundle cannot be installed using the NSP Artifacts function.

Note: Only RSA format is currently supported, using the PCKS standard. The use of any other format will result in a key that is not accepted by the NSP Artifacts function.

18.2.2 Steps

1

Log in as the root or NSP admin user on a Linux system where openssl is available.

2

Open a console window.

3

Enter the following to generate a private key:

```
# openssl genrsa -out private.pem 2048 ↵
```

4

Enter the following to create a public key:

```
# openssl rsa -in private.pem -pubout -out publickey.pem ↵
```

5

Enter the following to encode the public key in base64 format:

```
# cat public.pem | openssl base64 -e -A ↵
```

6

Designate a name to appear in the NSP UI as the name of the bundle author. Enter the following to encode the author name in base64:

```
# echo -n author name | openssl base64 ↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The **-n** after the echo command is mandatory: without it the author name contains a new line character and the verification of the signed bundles fails.

7

Enter the following to retrieve the Kubernetes name space of the artifact management application:

```
#  kubectl get pods -A | grep -i -e 'cam-server' -e 'NAMESPACE' ↵
```

The namespace value is output below the **NAMESPACE** heading.

8

Create a YAML file as shown in the sample below.

Configure the parameters:

- `author` is the encoded author name generated in Step 6
- `public-key` is the encoded public key value generated in Step 5
- `type` must be `public-key`
- `name` is the unique name for the public key
  Nokia recommends using the convention *`author name`*`-public-key` for easy recognition.
- `namespace` is the namespace retrieved in Step 7

Sample YAML:

```
apiVersion: v1
data:
  author:
  public key:
kind: Secret
metadata:
  labels:
    type: public-key
  name:
  namespace:
type: public-key
```

9

Enter the following to load the YAML file into the Kubernetes system:

```
#  kubectl -n namespace apply -f filename.yaml ↵
```

10

If applicable, transfer the YAML file to all standby sites and repeat Step 9 on each site.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Close the console window.

END OF STEPS

18.3 How do I manage public/private key pairs?

18.3.1 Commands

Use the following commands as needed to retrieve information and manage custom key information.

Keys owned by Nokia cannot be managed.

Viewing and saving key details

- To list existing public keys:

  # **kubectl get secrets -A | grep -i -e 'NAMESPACE' -e 'public-key'** ↵

  The output displays the namespace and the value of the `name` parameter in the secret file.
- To retrieve details of a public key:

  # **kubectl -n *namespace* get secrets *name* -o yaml** ↵

  where *namespace* and *name* are the namespace and the name of the public key, as displayed by the list command.
- To load the YAML file into the Kubernetes system:

  # **kubectl -n *namespace* apply -f *filename*.yaml** ↵

If a public key contains an invalid author name such as Nokia, the metadata includes the following line: `cam.additionalInfo: value of author is not valid`. If this line is present, a signature using this key is not valid.

Revoking a key

Only one public key can be in use per author. If a private key has been compromised and a new keypair is required, the old key must be revoked before the new key can be created and installed.

To revoke a key:

kubectl -n *namespace* delete secrets *name* -o yaml ↵

where *namespace* and *name* are the namespace and the name of the public key, as displayed by the list command.

If a key has been revoked and replaced, all artifact bundles that were signed with the old key must be signed again. Artifact bundles that are already installed are not affected.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

19 Telemetry administration

19.1 What is telemetry administration?

19.1.1 Description

Telemetry administration consists of managing files and options required for cloud native (CN) telemetry.

19.2 Process to enable CN telemetry

19.2.1 Purpose

Use this procedure to set up CN telemetry on NSP. Some steps in this procedure are only required if third-party NEs are in use.

19.2.2 Deploy CN telemetry

1

Open a terminal session to the NSP deployer VM

2

Log in as the root or NSP admin user.

3

Enable the GNMI Telemetry and Accounting Telemetry installation options in the NSP deployment as needed; see 11.4 “How do I update the NSP system configuration?” (p. 340).

19.2.3 Upgrade adaptors to 25.8 or later

Adaptors from releases earlier than 23.11 must be upgraded to use CN telemetry.

1

Obtain the new adaptor adaptation bundle from the Nokia NSP software delivery site, in the NSP/<release>/Artifacts folder.

2

Install the new adaptor adaptation bundle, see “How do I install an artifact bundle?” in the *NSP Network Automation Guide*.

Note: it is not necessary to remove the older adaptors when upgrading.

3

See the artifact guides for your NEs for any additional required steps.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

19.2.4 Enable TLS

1

Transfer the TLS certificate file for each NE to the following directory on the NSP deployer VM:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/tls/telemetry

See the NE documentation for information about generating NE TLS certificate files.

2

Enter the following to apply the certificates:

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy↵
```

Do not modify or delete files in this directory.

19.2.5 Check the Telemetry Statistic Search Tool

CN telemetry is enabled for gNMI and accounting collection. You can verify the availability of the telemetry types you need in the Telemetry Statistic Search Tool.

1

Open the Telemetry Statistic Search Tool and search for your desired telemetry types.

If you do not find the definition or mapping you require, or you need to augment an existing telemetry type, contact your Nokia service representative.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20 NSP auxiliary database administration

20.1 What is an NSP auxiliary database?

20.1.1 Description

An NSP auxiliary database provides additional statistics data storage, and is required for advanced storage and retrieval for functions such as NSP Analytics. An auxiliary database is deployed on one station, or as a cluster of three or more stations, depending on the scale requirements.

Auxiliary database deployment also supports geographically redundant, or geo-redundant, deployment using functionally identical auxiliary database clusters in separate data centers.

An NSP operator uses a RESTCONF API call to return the auxiliary database status, as described in 20.5 “How do I check the auxiliary database status?” (p. 527).

20.1.2 Auxiliary database fault tolerance

The following provide auxiliary database fault tolerance:

- hardware redundancy, in a multi-station cluster
- geographically redundant clusters; see “Geo-redundant deployment” (p. 521)
- data replication among the stations in a multi-station cluster, and between clusters in a geo-redundant deployment
- manual and scheduled database backups

Hardware redundancy

If enough members of an auxiliary database cluster fail, the cluster is considered to be failed, and an alarm is raised. When a geo-redundant cluster fails, the local NSP cluster initiates an auxiliary database switchover, and the standby cluster assumes the primary role.

In order for a cluster to be considered failed, the number of unavailable cluster members varies by the cluster size:

- one-member cluster—one
- three-or-more-member cluster—two

Geo-redundant deployment

Auxiliary database deployment supports geo-redundancy, in which an auxiliary database cluster is deployed in each data center of a DR NSP deployment.

The auxiliary database cluster that has the primary role processes transactions and replicates the data to the standby cluster every 30 minutes.

In the event that the primary auxiliary database cluster is unreachable, the standby cluster initiates a database failover and assumes the primary role. The failover function is independent of NFM-P or NSP system redundancy functions, and is non-revertive. 16.3 “How do I perform an auxiliary

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

database switchover?" (p. 533) describes how to switch the auxiliary database cluster roles in a DR deployment, which may be required after a failover to restore the initial primary and standby cluster roles.

For more information about auxiliary database redundancy, see 16.2.1 "Auxiliary database geographic redundancy" (p. 459).

Note: During some internal operations, the status of one or more standby cluster members may be UNREACHABLE temporarily, and is no cause for concern.

Backups and restores

An auxiliary database backup operation backs up the database data on each auxiliary database station in the primary cluster. Scheduled backups are strongly recommended.

Note: Scheduled auxiliary database backups are disabled by default; see 20.7 "How do I schedule auxiliary database backups?" (p. 531) and 20.8 "How do I manually backup the auxiliary database?" (p. 532) for information.

Although an auxiliary database may be distributed among multiple stations, a database restore operation is initiated on one station, and automatically replicates the restored data among the other stations, as required.

See 20.10 "How do I restore an auxiliary database?" (p. 533) for information.

Fault detection

To detect a database failure or a connectivity loss, the local NFM-P main server or NSP cluster monitors each station in the primary auxiliary database cluster. If a failure is detected, the NSP raises one of the following major or critical alarms, which are not self-clearing unless otherwise noted:

- cluster member unavailable
- database unavailable
- for geo-redundancy:
  - database proxy down (self-clearing)
  - primary cluster unreachable
  - cluster copy failure
  - activation failure
  - activation triggered.
  - standby cluster unreachable

Note: The geo-redundancy alarms are NSP alarms, so are not reported by the NFM-P. The alarm information is available to subscribers of the Kafka FAULT topic, and to RESTCONF API clients, but not to NFM-P XML API clients.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.2 How do I collect NSP log files?

20.2.1 NSP auxiliary database

If required, use a script to collect a comprehensive set of log files.

1

Log in to the station as the root user.

2

Open a console window.

3

Enter the following:

- On an auxiliary database station:
  # **/opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles *output_dir days*** ↵
  where
  output_dir is a local directory that is to contain the output files
  days is the optional number of days for which to collect log files

Note: You cannot specify /tmp, or any directory below /tmp, as the output directory.

4

Collect the output files:

- *hostname_date*.WsInfoFiles.*checksum*.tar.gz
  Contains station-specific information such as the hardware and network configuration
- *hostname_date*.ServerLogFiles.*checksum*.tar.gz
  Contains server and JBoss logs, and configuration information
- *hostname_date*.DBLogFiles.*checksum*.tar.gz
  Contains NFM-P database logs and configuration information

End of steps

20.3 How do I start an auxiliary database cluster?

20.3.1 Purpose

Perform this procedure to start the auxiliary database software on all stations in an auxiliary database cluster, for example, after maintenance.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1

Log in to an auxiliary database station as the root user.

2

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

3

Enter the following:

```
# ./auxdbAdmin.sh start ↵
```

4

The auxiliary database starts.

5

If the auxiliary database proxies were stopped or the shields were raised in order to block external access to the auxiliary database ports, start the proxies and lower the shields by performing the following:

```
# ./auxdbAdmin.sh startAndEnableServices ↵
```

6

Enter the following to display the auxiliary database status:

```
# ./auxdbAdmin.sh status ↵
```

Information like the following is displayed:

```
Database status
Node       | Host          | State | Version | DB
-----------+---------------+-------+---------+-------
node_1     | internal_IP_1 | STATE | version | db_name
node_2     | internal_IP_2 | STATE | version | db_name
...
node_n     | internal_IP_n | STATE | version | db_name
      Output captured in log_file
```

The cluster is started when each *STATE* entry reads UP.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.4 How do I stop an auxiliary database cluster?

20.4.1 Purpose

CAUTION

Service disruption

Stopping an auxiliary database cluster may be service-affecting.

Perform the procedure only if required, and only during a scheduled maintenance period.

Note: In a geo-redundant auxiliary database, stopping the primary cluster will cause the standby cluster to be activated. If this behaviour is not desired, you must stop the auxiliary database proxy on the standby auxiliary database stations first.

If you do not know which cluster is currently the primary cluster, perform 20.5 “How do I check the auxiliary database status?” (p. 527).

Perform this procedure to stop the auxiliary database software on all stations in an auxiliary database cluster, for example, for maintenance purposes.

1

If the NSP deployment does not include the NFM-P, go to Step 4.

2

Perform the following steps on each NFM-P auxiliary server station to stop the server.

1. Log in to the station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/auxserver/nms/bin ↲
   ```

4. Enter the following:

   ```
   bash$ ./auxnmsserver.bash auxstop ↲
   ```

5. Enter the following to display the auxiliary server status:

   ```
   bash$ ./auxnmsserver.bash auxappserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Auxiliary Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

3

Perform the following steps on each NFM-P main server station to stop the server.

Note: In a redundant system, you must perform the steps on the standby main server first.

1. Log in to the station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following to display the NFM-P server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

4

Log in to any auxiliary database station in the cluster as the root user.

5

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

6

Enter the following to stop and disable the auxiliary database services:

```
# ./auxdbAdmin.sh stopAndDisableServices ↵
```

7

Enter the following:

```
# ./auxdbAdmin.sh stop ↵
```

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial
setup for auxiliary database, press enter]:
```

8

Enter the dba password.

Information like the following is displayed:

```
Database samdb stopped successfully
Database status
Node       | Host          | State | Version | DB
-----------+---------------+-------+---------+-------
node_1     | internal_IP_1 | STATE | version | db_name
node_2     | internal_IP_2 | STATE | version | db_name
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
...
node_n      | internal_IP_n | STATE | version | db_name
  Output captured in log_file
```

Note: If the inital stop does not succeed, force_stop is attempted automatically until the auxiliary database is stopped. If the database does not stop, do not proceed to the next step and contact Nokia support for further assistance.

9

Close the console windows.

END OF STEPS

20.5 How do I check the auxiliary database status?

20.5.1 Purpose

Perform the following procedures to obtain the status of the auxiliary database clusters in an NSP deployment through RESTCONF APIs or the NSP UI.

20.5.2 Steps

Check the auxiliary database status from the NSP UI.

1

As an NSP administrator, choose **System Health** from the NSP main menu.

2

View the information in the Auxiliary Database Clusters panel, which lists the following:

- Backup status
  - Scheduled backup—whether backups are enabled
  - Next backup—date and time
  - Last backup—date and time when the last backup started. This field indicates whether the backup is scheduled or manual. The status of the last backup is displayed only if it fails.
- Clusters
  - Status and cluster name—the dot beside the name shows the cluster status
  - Role—active or standby
  - Status—whether the cluster is up
  - Alarms—number of alarms per type

To view expanded details for a cluster, click **Show nodes** below the cluster details to display the following:

- Status and IP address or cluster name—the dot beside the IP address or name of the cluster shows the cluster status
- Node status—whether the node is up

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- Proxy status—whether the auxiliary database proxy is up
- Internal address—internal cluster address

END OF STEPS

20.5.3 Steps

Check the current status of the auxiliary database clusters from RESTCONF APIs.

1

Log in to a station that has access to the NSP system.

2

Open a console window.

3

Issue the following RESTCONF API call:

Note: In order to issue a RESTCONF API call, you require a token; see the My First NSP API Client tutorial on the Network Developer Portal for information.

`GET https://address/restconf/data/auxdb:clusters`

where *address* is the NSP advertised address

The call returns auxiliary database cluster status information like the following:

```
{
    "clusters": {
        "cluster": [
            {
                "name": "cluster_1",
                "mode": "ACTIVE",
                "status": "UP",
                "secure": true,
                "nodes": [
                    {
                        "external-ip": "203.0.113.101",
                        "internal-ip": "10.1.2.101",
                        "status": "UP"
                    },
                    {
                        "external-ip": "203.0.113.102",
                        "internal-ip": "10.1.2.102",
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
                            "status": "UP"
                        },
                        {
                            "external-ip": "203.0.113.103",
                            "internal-ip": "10.1.2.103",
                            "status": "UP"
                        }
                    ]
                },
                {
                    "name": "cluster_2",
                    "mode": "STANDBY",
                    "status": "ON_STANDBY",
                    "secure": true,
                    "nodes": [
                        {
                            "external-ip": "203.0.113.104",
                            "internal-ip": "10.1.2.104",
                            "status": "READY"
                        },
                        {
                            "external-ip": "203.0.113.105",
                            "internal-ip": "10.1.2.105",
                            "status": "READY"
                        },
                        {
                            "external-ip": "203.0.113.106",
                            "internal-ip": "10.1.2.106",
                            "status": "READY"
                        }
                    ]
                }
            ]
        }
    }
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

View each status value.

Note: The *cluster_1* and *cluster_2* addresses correspond to the ipList and standbyIpList parameter values in the **auxDb** section of the NSP cluster configuration file.

5

If each status value of the standby cluster nodes is not READY, contact technical support.

Each status value of the active cluster nodes is expected to be UP.

6

Close the console window.

END OF STEPS

20.6 How do I change the samauxdb RHEL user password?

20.6.1 Purpose

Perform this procedure to change the password of the samauxdb RHEL user on an auxiliary database station.

Note: You must set the password to the same value on each auxiliary database station.

20.6.2 Steps

1

Log in to the auxiliary database station as the samauxdb user.

2

Open a console window.

3

Enter the following:

```
$ passwd ↵
```

The following prompt is displayed:

```
New Password:
```

4

Enter the new password and press ↵.

The following prompt is displayed:

```
Confirm New Password:
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Enter the new password again and press ↵. The password is changed.

6

Record the new password and store it in a secure location.

7

Close the console window.

8

Log out of the station.

END OF STEPS

20.7 How do I schedule auxiliary database backups?

20.7.1 Purpose

Perform this procedure to setup regular, scheduled backups of the NSP auxiliary database.

A backup operation can be scheduled to occur while a copy cluster operation is in process. In this case, the backup operation would wait until after the copy cluster operation is complete; the Auxiliary Database Clusters dashlet would display “Backing up...” to indicate that the backup is waiting to start.

An auxiliary database backup cannot be scheduled to occur while an auxiliary database switchover is in progress.

Note: If auxiliary database backups were previously scheduled in NFM-P, those scheduled backups will need to be recreated using this procedure.

20.7.2 Steps

1

Open System Health.

2

In the Auxiliary Database Clusters dashlet, click ···**More**, **Configure Backups**.

3

In the Configure Auxiliary Database Backups form, configure the backup scheduling and storage parameters.

The Backup Location is created if it does not exist already.

Note: If the following conditions are not met an error will occur:

1. The samauxdb user must have Read/Write permissions for the parent directory of the

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Backup Location on all auxiliary database stations in the cluster.

2. If the Backup Location already exists, the samauxdb user must have Read/Write permissions for the Backup Location on all auxiliary database stations in the cluster.

4

If you want to perform a database backup immediately, enable the **Backup on Save** option.

END OF STEPS

20.8 How do I manually backup the auxiliary database?

20.8.1 Purpose

Perform this procedure to start a manual, one-time backup of the NSP auxiliary database.

A manual auxiliary database backup operation can not be started when an auxiliary database backup is already in progress.

20.8.2 Steps

1

Open System Health.

2

In the Auxiliary Database Clusters dashlet, click ···**More**, **Backup Now**.

3

You are prompted to start the database backup. Click **Proceed**.

4

The backup starts. When it finishes, the Last Backup parameter displays the completion date and time, flagged as Manual.

Depending on the size of the auxiliary database, the backup can take several minutes.

END OF STEPS

20.9 How do I check the auxiliary database backup status?

20.9.1 Purpose

Perform this procedure to learn the status of the most recently invoked auxiliary database backup.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.9.2 Steps

1

Log in to a station that has access to the NSP cluster.

2

Open a console window.

3

Issue the following RESTCONF API call:

Note: In order to issue a RESTCONF API call, you require a token; see the My First NSP API Client tutorial on the Network Developer Portal for information.

`GET https://address/restconf/data/nsp-auxdb-backup:status`

where *address* is the NSP advertised address

The response includes the auxiliary database backup status.

4

View the status, which is one of the following:

- never_run—no initial backup performed
- running—backup in progress
- failed—backup attempt unsuccessful
- success—backup completed successfully
- unknown—status unavailable

5

If the status value is failed or unknown, contact technical support to investigate.

6

Close the console window.

END OF STEPS

20.10 How do I restore an auxiliary database?

20.10.1 Purpose

Perform this procedure to restore an auxiliary database from an auxiliary database backup file set.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

CAUTION

Service Disruption

Restoring an auxiliary database in a deployment that includes the NFM-P requires a shutdown of the NFM-P system and causes a network management outage.

Ensure that you perform this procedure only during a scheduled maintenance period.

20.10.2 Steps

Stop auxiliary database proxies

1

Log in as the root user on any station in the auxiliary database cluster.

Note: In a geo-redundant auxiliary database, you must stop the auxiliary database services on a station in both the primary and standby clusters, starting with a standby cluster's auxiliary database station.

2

Enter the following to stop and disable the auxiliary database services:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh stopAndDisableServices
↲
```

3

If the NSP deployment does not include the NFM-P, go to Step 6.

Stop NFM-P main and auxiliary servers

4

If the NFM-P system is redundant, stop the standby main server and the associated auxiliary servers.

1. Perform 21.7 “How do I stop an auxiliary server?” (p. 597) to stop each Preferred and Reserved auxiliary server of the standby main server.
2. Log in to the standby main server as the nsp user.
3. Open a console window.
4. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

5. Enter the following to stop the main server:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

6. Enter the following to display the main server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The server status is displayed; the server is fully stopped if the status is the following:

```
Application Server is stopped
```

If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

5

Stop the standalone or primary main server and the associated auxiliary servers.

1. Perform 21.7 “How do I stop an auxiliary server?” (p. 597) to stop each Preferred and Reserved auxiliary server of the primary or standalone main server.
2. Log in to the main server station as the nsp user.
3. Open a console window.
4. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

5. Enter the following to stop the main server:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

6. Enter the following to display the main server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Prepare auxiliary database stations

6

If the auxiliary database is geo-redundant, you must identify which auxiliary database cluster is currently primary.

If you do not know which cluster is currently the primary cluster, perform 20.5 “How do I check the auxiliary database status?” (p. 527).

7

Stop the standalone or primary auxiliary database.

Note: In a geo-redundant auxiliary database, you must ensure that each auxiliary database cluster is stopped before you attempt to perform a restore operation.

1. Log in as the root user on any station in the standalone or primary auxiliary database cluster.
2. Enter the following:

   ```
   # cd /opt/nsp/nfmp/auxdb/install/bin ↲
   ```

3. Enter the following to stop the auxiliary database:

   ```
   # ./auxdbAdmin.sh stop ↲
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

You are prompted to enter the database administrator user's password.

4. Enter the password. The auxiliary database stops.

   Information like the following is displayed:

```
Database samdb stopped successfully
Database status
Node       | Host          | State | Version | DB
-----------+---------------+-------+---------+-------
node_1     | internal_IP_1 | STATE | version | db_name
node_2     | internal_IP_2 | STATE | version | db_name
...
node_n     | internal_IP_n | STATE | version | db_name
  Output captured in log_file
```

   Note: If the inital stop does not succeed, force_stop is attempted automatically until the auxiliary database is stopped. If the database does not stop, do not proceed to the next step and contact Nokia support for further assistance.

8

If the backup files to restore are not in the original backup location on each auxiliary database station, perform the following steps.

1. If you know the original backup location, go to substep 6.
2. Open the following file for viewing:

   path/AuxDbBackUp/samAuxDbBackup_restore.conf

   where *path* is the current location of the backup file set
3. Locate the [Mapping] section, which contains one line like the following for each auxiliary server station:

   `v_name_node0001 = IP_address:path/AuxDbBackUp`

   The *path* is the original backup location.
4. Record the original backup location.
5. Close the samAuxDbBackup_restore.conf file.
6. Copy the AuxDbBackUp directory contents from the current backup location to the AuxDbBackUp directory in the original backup location on each auxiliary database station.
7. As the root user, enter the following command on each auxiliary database station:

   `# chown -R samauxdb path` ↵

   where *path* is the absolute path of the original backup location

9

If the backup is being restored on any stations that have different internal IP addresses, perform the following steps on each auxiliary database station.

1. Open the following file using a plain-text editor such as vi:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

path/AuxDbBackUp/samAuxDbBackup_restore.conf

where *path* is the location of the backup file set

2. Add the following internal mapping section to the end of the file; the example below is for an auxiliary database of three stations:

```
[NodeMapping]
v_name_node0001 = IP_address_1
v_name_node0002 = IP_address_2
v_name_node0003 = IP_address_3
```

where

v_*name*_node000*n* is the station name shown in the [Mapping] section of the file

IP_address_n is the new internal IP address of the station

3. Save and close the samAuxDbBackup_restore.conf file.

Perform auxiliary database restore operation

10

As the root user, enter the following on one auxiliary database station:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

11

Perform one of the following.

a. Restore the latest backup; enter the following:

```
# ./auxdbAdmin.sh restore path/AuxDbBackUp/samAuxDbBackup_restore.
conf ↵
```

where *path* is the original backup directory

b. Restore a backup other than the latest; perform the following steps.

1. Enter the following:

```
# ls path/AuxDbBackUp/.auxdb_backup_history ↵
```

where *path* is the original backup directory

The directory contents are listed; the following files are present for each previous backup:

- AuxDbBackUp*ID*_*datestamp*_*timestamp*_samAuxDbBackup_info.txt
- AuxDbBackUp*ID*_*datestamp*_*timestamp*_samAuxDbBackup_restore.txt

where

datestamp is the backup date, in the form *YYYYMMDD*

timestamp is the backup time, in the form *hhmmss*

ID is a unique numerical identifier

2. Based on the date and time of the backup that you want to restore, identify and record the *ID*, *datestamp*, and *timestamp* values.
3. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

./auxdbAdmin.sh restore *path*/AuxDbBackUp/.auxdb_backup_history/AuxDbBackUp*ID_datestamp_timestamp*_samAuxDbBackup_restore.conf ↵

where

path is the original backup directory

ID is the recorded *ID* value

datestamp is the recorded *datestamp* value

timestamp is the recorded *timestamp* value

The restore operation begins. The following messages and progress indicators are displayed:

```
Starting auxiliary database restore...
Starting full restore of database db_name.
Participating nodes: node_1, node_2, ... node_n.
Restoring from restore point: AuxDbBackUpID_datestamp_timestamp
Determining what data to restore from backup.
[==========================================] 100%
Approximate bytes to copy: nnnnnnnn of nnnnnnnnn total.
Syncing data from backup to cluster nodes.
```

When the restore is complete, the second progress indicator reaches 100%, and the following message is displayed:

```
[==========================================] 100%
Restoring catalog.
Restore complete!
```

Once the restore is complete, the database will start and post-restore configuration will be performed.

```
Vertica restore completed. Starting the database.
Info: no password specified, using none
Going with traditional slower startup
Starting nodes:
  v_samdb_node0001 (IP_a)
  .
  .
  .
Database samdb: Startup Succeeded.  All Nodes are UP
```

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial
setup for auxiliary database, press enter]:
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12

Enter the database administrator password recorded during creation of the backup.

Post-restore configuration output appears on the console, followed by:

```
  Output captured in /opt/nsp/nfmp/auxdb/install/log/auxdbAdmin.sh.
timestamp.log
```

13

Enter the following to configure TLS settings:

```
# ./auxdbAdmin.sh configureTLS ↵
```

Restore database user passwords

14

If a database user password has changed since the creation of the database backup, the NSP components cannot authenticate with the restored auxiliary database.

In such a scenario, you must perform the following steps to update each affected database user password to the value that the NSP components recognize.

1. Enter the following on the current auxiliary database station to connect to the auxiliary database:

   ```
   # su - samauxdb ↵
   # vsql ↵
   ```

   You are prompted for credentials.

2. Enter the following:
   - user—samauxdb
   - password—database administrator password recorded during creation of backup

3. Enter the following once for each user whose password has changed since the backup creation:

   ```
   ALTER USER user IDENTIFIED BY 'password'; ↵
   ```

   where

   user is the database user name

   password is the newer password recognized by the NSP

4. Exit vsql:

   ```
   # \q ↵
   ```

5. Enter the following with each affected user to verify the success of the password change:

   ```
   # vsql -U user -c '\echo success' ↵
   ```

   Enter the newer password for the user.

   Confirm that the word "success" appears on the console.

6. Enter the following to switch back to the root user:

   ```
   # exit ↵
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7. Ensure that the NSP components are able to connect to the auxiliary database.

Start auxiliary database proxies

15

Enter the following to enable and start the auxiliary database services:

```
# ./auxdbAdmin.sh startAndEnableServices ↵
```

Note: In a geo-redundant auxiliary database, you must start the proxy on the stations of the restored auxiliary database cluster first.

16

If the NSP deployment does not include the NFM-P, go to Step 19.

Start NFM-P servers

17

Start the standalone or primary main server and associated auxiliary servers.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following to start the main server:

   ```
   bash$ ./nmsserver.bash start ↵
   ```

5. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

6. Perform 21.6 “How do I start an auxiliary server?” (p. 596) to start each Preferred and Reserved auxiliary server of the primary or standalone main server.

18

If the NFM-P system is redundant, start the standby main server and associated auxiliary servers.

1. Log in to the standby main server as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4. Enter the following to start the main server:

   ```
   bash$ ./nmsserver.bash start ↵
   ```

5. Enter the following to display the main server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

6. Perform 21.6 “How do I start an auxiliary server?” (p. 596) to start each Preferred and Reserved auxiliary server of the standby main server.

19

Close the open console windows.

END OF STEPS

20.11 How do I change an auxiliary database user password?

20.11.1 Before you begin

Note: If a geo-redundant auxiliary database switchover occurs before the next database copy cluster completes (run every 30 minutes), the user password will need to be changed again because the newly-activated primary database will still have the old password.

20.11.2 Purpose

1

Log in to a station that has access to the NSP cluster.

2

Open a console window.

3

Issue the following RESTCONF API call:

Note: In order to issue a RESTCONF API call, you require a token; see the My First NSP API Client tutorial on the Network Developer Portal for information.

POST https://*address*/restconf/data/nsp-auxdb-user:users/user=*username*/change-password

where

address is the NSP advertised address

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

username is the username, for example, samauxdb, samuser, samanalytic, or samanalytic_ano

The request body is the following, in which you specify the new and current passwords:

```
{
    "nsp-auxdb-user:input" : {
        "new-password": "new_password",
        "current-password": "current_password"
    }
}
```

The following is an example of a success response:

```
{
    "nsp-auxdb-user:output": {},
    "statusCode": "OK"
}
```

4

Close the console window.

END OF STEPS

20.12 How do I change the auxiliary database external IP addresses?

20.12.1 Purpose

Perform this procedure when the IP addresses that an auxiliary database uses to communicate with other NSP components must change, for example, when the auxiliary database moves to a different subnet, or when the protocol in use by the NSP components changes from IPv4 to IPv6.

Note: Changing the internal IP addresses of the auxiliary database cluster members is not supported.

20.12.2 Steps

Stop NFM-P main servers, auxiliary database

1

If the NSP deployment does not include the NFM-P, go to Step 3.

2

Perform the following steps on each NFM-P main server station to stop the server.

Note: In a redundant system, you must perform the steps on the standby main server first.

1. Log in to the station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following to display the NFM-P server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

3

Perform the following steps on each auxiliary database station.

1. Log in to the station as the root user.
2. Open a console window.
3. Open the /etc/hosts file using a plain-text editor such as vi.
4. Change the IP address that is mapped to the station hostname to the new IP address associated with the hostname.

Reconfigure addresses

4

Log in to one of the auxiliary database stations as the root user.

5

Enter the following to stop and disable the auxiliary database services:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh stopAndDisableServices
↵
```

6

Open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

CAUTION

Service disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the steps, without guidance from technical support.

Locate the following line and change each *export_IP* value to the new IP address:

export_hosts=*internal_IP1*[*export_IP1*],*internal_IP2*[*export_IP2*]...*internal_IPn*[*export_IPn*]

8

Save and close the install.config file.

9

Enter the following on the same station:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh updateInterfaces ↵
```

The following prompt is displayed.

```
Please enter auxiliary database administrator user's password [if you
are doing initial setup for auxiliary database, press enter]:
```

10

Enter the password.

Messages like the following are displayed.

```
Dropping host public interfaces for 10.1.2.105
  Dropped interface PUBLIC_IF_10_1_2_105 on node v_samdb_node0001.
Creating public interface for host 10.1.2.105[new_external_address]
Dropping host public interfaces for 10.1.2.106
  Dropped interface PUBLIC_IF_10_1_2_106 on node v_samdb_node0002.
Creating public interface for host 10.1.2.106[new_external_address]
Dropping host public interfaces for 10.1.2.107
  Dropped interface PUBLIC_IF_10_1_2_107 on node v_samdb_node0003.
Creating public interface for host 10.1.2.107[new_external_address]
Distributing install.config to all nodes
  Output captured in /opt/nsp/nfmp/auxdb/install/log/auxdbAdmin.sh.
timestamp.log
```

11

Enter the following to enable and start the auxiliary database services:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh startAndEnableServices
↵
```

Update NFM-P main servers

12

If the NSP deployment does not include the NFM-P, go to Step 14.

13

Perform the following steps on each main server station.

1. Log in to the main server station as the root user.
2. Open a console window.
3. Enter the following:

   ```
   # samconfig -m main ↵
   ```

4. Enter the following:

   ```
   <main> configure auxdb ip-list address1,address2...addressN exit ↵
   ```

   where *address1*,*address2*...*addressN* are the new IP addresses of the auxiliary database stations

   Note: For geo-redundant auxiliary database clusters, each cluster is specified with comma-separated IP addresses as shown above, however a semicolon is used to delimit the two clusters.

5. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

6. Enter the following:

   ```
   <main> exit ↵
   ```

   The samconfig utility closes.

Reconfigure NSP clusters

14

Perform Step 15 to Step 21 on the NSP cluster in each data center.

15

Stop the NSP cluster.

Note: In a standalone deployment, performing this step marks the beginning of the service outage.

1. Open a terminal session to the NSP deployer VM.
2. Log in as the root or NSP admin user.
3. Open the following file using a plain-text editor such as vi:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

4. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```

5. Save and close the file.
6. Enter the following:

   # cd /opt/nsp/NSP-CN-DEP-*release-ID*/bin ↵
7. Enter the following:

   # ./nspdeployerctl uninstall --undeploy ↵

   The NSP cluster stops.

16

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

17

Locate the following section:

```
auxDb:
  ipList: "cluster_1_IP1,cluster_1_IP2...cluster_1_IPn"
  standbyIpList: "cluster_2_IP1,cluster_2_IP2...cluster_2_IPn"
```

18

Edit the IP addresses as required.

19

Save and close the file.

20

Enter the following to start the NSP cluster:

/opt/nsp/NSP-CN-DEP-*release-ID*/bin/nspdeployerctl install --config --deploy ↵

The NSP cluster starts, and the configuration update is put into effect.

21

Close the console window.

Start NFM-P main servers

22

If the NSP deployment does not include the NFM-P, go to Step 24.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

23

Perform the following steps on each main server station to start the main server.

Note: In a redundant system, you must start the primary main server first.

1. Return to the open console window on the main server station.
2. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↵
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

24

Close the open console windows.

END OF STEPS

20.13 How do I test auxiliary database disk performance?

20.13.1 Purpose

The disk performance of an NFM-P component affects overall system performance, and must meet or exceed the minimum specifications in the response to the NFM-P Platform Sizing Request for your system.

Also, before you add capacity to a disk or partition on an NFM-P component, for example, using LVM, you must ensure that the disk throughput and latency values remain within tolerance, which is defined as being within 10% of the current values.

Note: The disk performance of the stations in an auxiliary database cluster must be closely matched. You must test and compare the disk performance of each station in a cluster to ensure optimal performance.

Perform this procedure to check the disk performance of an NSP auxiliary database station.

CAUTION

Service Disruption

Checking the disk performance requires a shutdown of the auxiliary database cluster and is service-affecting.

Perform the procedure only during a scheduled maintenance period.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.13.2 Steps

1

Perform 20.4 “How do I stop an auxiliary database cluster?” (p. 525).

2

When the auxiliary database cluster is stopped, enter the following as the root user on the auxiliary database station to begin the test:

```
# /opt/vertica/bin/vioperf /opt/nsp/nfmp/auxdb/data ↵
```

3

Record the utility output.

4

As a routine performance check, perform the following steps.

1. Compare the following recorded values with the values specified for your auxiliary database deployment:
   - Read
   - Write
   - Rewrite
   - %IO Wait
2. If the values do not meet the minimum specifications, contact technical support.
3. Go to Step 6.

5

If you are adding capacity to a disk or partition, perform the following steps.

1. Add the required capacity to the disk or partition.
2. Repeat Step 2 and Step 3 as required.
3. Compare the following values from before and after the capacity increase:
   - Read
   - Write
   - Rewrite
   - %IO Wait
4. If the values differ by more than 10%, contact technical support.

6

Close the console windows.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.14 How do I add an auxiliary database station?

20.14.1 Purpose

The following steps describe how to add a new station to an auxiliary database, for example, to accommodate network growth.

To perform his procedure, the RHEL 9 OS must be installed on the auxiliary database station.

CAUTION

Service Disruption

This procedure requires a restart of each NFM-P main server, so is service-affecting.

Perform this procedure only during a scheduled maintenance period.

Note: You cannot add a station to a one-station auxiliary database.

Note: The primary and standby auxiliary database clusters in a geo-redundant deployment require the same number of stations.

Note: Nokia recommends enabling password-free SSH between auxiliary database cluster hosts for the root user.

20.14.2 Steps

Install software

1

Add a hostname entry for the new station to the /etc/hosts file on each existing auxiliary database station.

Note: The hostname must be the fully qualified hostname, and not the short hostname.

Note: Hostnames are case-sensitive.

2

Log in as the root user on the new auxiliary database station.

3

Add a hostname entry for the new station to the /etc/hosts file on the new station using the following criteria.

- The first entry for the station hostname in the file must be the station IP address that is reachable by each main server and NSP cluster.
- The hostname must be the fully qualified hostname, and not the short hostname.
- The hostname must:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- contain only ASCII alphanumeric and hyphen characters.
- not begin or end with a hyphen.
- not begin with a number.
- comply with the format defined in IETF RFC 1034.
- use period characters delimit the FQDN components.
- not exceed 63 characters.

Note: Hostnames are case-sensitive.

4

Download the following installation files to an empty local directory:

Note: You must ensure that the directory is empty.

Note: The software release must match the software release of the existing auxiliary database.

- nspos-auxdb-*R.r.p*-rel.*v*.rpm
- VerticaSw_PreInstall.sh
- nspos-jre-*R.r.p*-rel.*v*.rpm
- vertica-*R.r.p*-rel.tar

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version number

Note: In subsequent steps, the directory is called the software directory.

5

Open a console window.

6

Navigate to the software directory.

Note: The directory must contain only the installation files.

7

Enter the following:

chmod +x * ↵

8

Enter the following:

./VerticaSw_PreInstall.sh ↵

The script displays configuration messages like the following, and a prompt:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Logging Vertica pre install checks to log_file
INFO: About to set proxy parameters in /etc/profile.d/proxy.sh...
INFO: Completed setting proxy parameters in /etc/profile.d/proxy.sh...
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
conf...
INFO: Backing up /etc/logrotate.conf to /etc/logrotate.conf.orig
INFO: Removing /var/log/wtmp entry from /etc/logrotate.conf
INFO: Adding /etc/logrotate.d/wtmp
Checking user group nsp...
Adding user group nsp...
Checking user nsp...
Adding nsp...
Checking Linux user group samauxdb...
Adding user group samauxdb...
Checking user samauxdb...
Adding samauxdb...
Set password for samauxdb... New password:
```

9

Enter a password that conforms to the RHEL password criteria.

The following prompt is displayed:

```
Retype new password:
```

10

Re-enter the password.

Messages like the following are displayed:

```
Changing password for user samauxdb.
passwd: all authentication tokens updated successfully.
Adding samauxdb to /etc/cron.allow
Moving logfile from /tmp ...
     ... to /opt/nsp/nfmp/auxdb/install/log
Changing ownership of the directory /opt/nsp/nfmp/auxdb/install to
samauxdb:samauxdb.
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Removing group write and world permissions from the directory
/opt/nsp/nfmp/auxdb/install.
Appending Vertica section to /opt/nsp/nfmp/auxdb/install/.bashrc ...
Creating /opt/nsp/nfmp/auxdb/data for Vertica database files.
Changing ownership of /opt/nsp/nfmp/auxdb files.
INFO: Creating auxiliary database prep script.
INFO: Creating nspos-auxdb-prep systemd service.
INFO: Enabling nspos-auxdb-prep systemd service.

************************************************************************
* *
* Changes were made that require a restart. *
* Please restart this host before proceeding with Vertica
installation. *
* *
************************************************************************
```

11

Perform the following steps to restart the station.

1. Enter the following:

   # **systemctl reboot** ↵

   The station restarts.
2. Log in to the station as the root user.
3. Open a console window.
4. Navigate to the software directory.

12

Enter the following:

tar xvf vertica-R.r.p-rel.tar $(tar tf vertica-R.r.p-rel.tar | sort -V | tail -1) ↵

13

Enter the following:

dnf install *.rpm ↵

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

14

Enter y. The following and the installation status are displayed as each package is installed:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Downloading Packages:
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

Add new station to auxiliary database configuration

15

When the package installation is complete, perform the following step as the root user on one of the auxiliary database stations to stop and disable the auxiliary database services:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh
stopAndDisableServices↵
```

Note: For a geo-redundant auxiliary database, the step must be performed on a station in each auxiliary database cluster.

16

Log in to an existing auxiliary database station as the root user.

Note: If the auxiliary database is geo-redundant, the station must be in the primary auxiliary database cluster.

17

Open a console window.

18

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

19

Enter the following:

```
# ./auxdbAdmin.sh addNode internal_IP external_IP ↵
```

where

internal_IP is the IP address from which the station communicates with the other auxiliary database stations

external_IP is the IP address from which the station communicates with other components in the deployment

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The script displays the following:

```
Adding hosts(s) hostname to auxiliary database cluster ...
```

20

You are prompted to enter the auxiliary database dba password.

Enter the samauxdb database administrator password.

21

You are prompted to enter the root user password for the new station.

Enter the password of the root user account on the new station.

22



CAUTION

Installation Failure

If the addition of the station to the auxiliary database is interrupted, the operation fails and support intervention may be required.

You must answer yes to the prompt described in this step.

If the auxiliary database contains a large amount of data, the addition of the station may take considerable time. In such a scenario, the following prompt is displayed:

```
Do you want to continue waiting? (yes/no) [yes]
```

Press ↵ to accept the default of yes.

Note: The prompt may be displayed several times during the operation.

23

When the script execution is complete, open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

24



CAUTION

Service Disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the step, without guidance from technical support.

Edit the following line in the file to read:

hosts=*internal_IP1*,*internal_IP2*...*internal_IPn*,*new_internal_IP*

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

where

internal_IP1,*internal_IP2*...*internal_IPn* are the IP addresses of the existing auxiliary database stations

new_internal_IP is the IP address from which the new station communicates with the other auxiliary database stations

25

Edit the following line in the file to read:

export_hosts=*internal_IP1*[*export_IP1*],*internal_IP2*[*export_IP2*]...*internal_IPn*[*export_IPn*],*new_internal_IP*[*new_export_IP*]

where

internal_IP1[*export_IP1*],*internal_IP2*[*export_IP2*],*internal_IPn*[*export_IPn*] are the IP addresses of the existing auxiliary database stations

new_internal_IP is the IP address from which the new station communicates with the other auxiliary database stations

new_export_IP is the IP address from which the new station communicates with the NFM-P servers

26

Save and close the install.config file.

27

Enter the following to generate certificates:

```
# ./auxdbAdmin.sh configureTLS ↵
```

Initialize auxiliary database

28

Enter the following:

```
# ./auxdbAdmin.sh distributeConfig ↵
```

The updated auxiliary database configuration is distributed to each auxiliary database station.

Rebalance cluster

29

Enter the following:

```
# ./auxdbAdmin.sh rebalance ↵
```

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial
setup for auxiliary database, press enter]:
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

30

Enter the database user password.

The following messages and prompt are displayed:

```
KSAFE factor of 1 detected

Rebalance was started in the background. Please don't reboot system
until rebalance is completed.

You can track the rebalance process by typing 'ps -fe | grep
rebalance'. Rebalance can take a very long time on large databases.
Please be patient.

Type YES to continue
```

31



CAUTION

Data corruption

Interrupting the rebalance operation can cause data corruption.

Do not interrupt the operation by, for example, rebooting the station.

Enter YES.

The rebalance operation begins, and the following is displayed:

```
Output captured in /opt/nsp/nfmp/auxdb/install/log/auxdbAdmin.sh.
timestamp.log
```

where *timestamp* is the start time of the rebalance operation

32

Monitor the rebalance operation; do not proceed to the next step until the operation is complete.

Note: A rebalance operation on a large database may take several hours.

Enter the following periodically to identify whether the rebalance process is active:

```
#  ps -ef | grep rebalance ↵
```

If the rebalance process is active, two lines of output are displayed. If the rebalance is complete, only one line like the following is displayed:

```
root     nnnnn  nnnn 0 hh:mm pts/0    00:00:00 grep --color=auto
rebalance
```

33

When the rebalance is complete, if the auxiliary database is not geo-redundant, go to Step 40.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Update standby auxiliary database configuration

34

Log in to an existing standby auxiliary database station as the root user.

35

Open a console window.

36

Perform Step 19 to Step 32.

37

Stop the standby auxiliary database; enter the following on an existing standby auxiliary database station:

```
# ./auxdbAdmin.sh stop ↵
```

The following prompt is displayed:

```
Please enter auxiliary database dba password [if you are doing initial
setup for auxiliary database, press enter]:
```

38

Enter the dba password.

Information like the following is displayed:

```
Database samdb stopped successfully
Database status
Node        | Host           | State | Version | DB
------------+----------------+-------+---------+-------
node_1      | internal_IP_1 | STATE | version | db_name
node_2      | internal_IP_2 | STATE | version | db_name
...
node_n      | internal_IP_n | STATE | version | db_name
  Output captured in log_file
```

Note: If the inital stop does not succeed, force_stop is attempted automatically until the auxiliary database is stopped. If the database does not stop, do not proceed to the next step and contact Nokia support for further assistance.

39

If the NSP deployment does not include the NFM-P, go to Step 43.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Configure NFM-P main servers

40



CAUTION

Misconfiguration Risk

If you alter the original IP-address assignments, or the order of the IP addresses, the station addition fails.

Do not change any of the original auxiliary database station IP address assignments, or the address order, in the main server configuration.

In a geo-redundant auxiliary database deployment, the order of the IP addresses must match in each main server configuration in each data center.

Perform the following steps on each main server station.

Note: In a geo-redundant system, you must perform the steps on the main servers in each data center.

Note: In a redundant system, you must perform the steps on the standby main server station first.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

5. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

6. Enter the following to switch to the root user:

   ```
   bash$ su ↲
   ```

7. Enter the following:

   ```
   # samconfig -m main ↲
   ```

   The following is displayed:

   ```
   Start processing command line inputs...
   <main>
   ```

8. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: For a geo-redundant auxiliary database, the order of the IP addresses must be the same on each main server in each data center.

```
<main> configure auxdb ip-list IP_list exit ↵
```

where

IP_list is a list of the IP addresses in the following format:

cluster_1_IP1,cluster_1_IP2,cluster_1_IPn,cluster_1_new_IP;cluster_2_IP1,cluster_2_IP2,cluster_2_IPn,cluster_2_new_IP

where *new_IP* is the external IP address of the new station

Note: The format example shows the new address added to cluster_1; cluster_2 addresses are present only for a geo-redundant auxiliary database. Ensure that you add *new_IP* to the address list for the appropriate cluster.

9. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

10. Enter the following:

    ```
    <main> exit ↵
    ```

    The samconfig utility closes.

11. Enter the following to switch back to the nsp user:

    ```
    # exit ↵
    ```

Start NFM-P main servers

41

On the standalone or primary main server station, enter the following to start the main server:

```
bash$ ./nmsserver.bash start ↵
```

The main server starts, and the station is added to the auxiliary database.

42

If the NFM-P system is redundant, enter the following on the standby main server station to start the main server:

```
bash$ ./nmsserver.bash start ↵
```

The main server starts.

Configure NSP clusters

43

Open a terminal session to the NSP deployer VM

44

Log in as the root or NSP admin user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

45

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/nsp-config.yml

46

Locate the following section:

```
auxDb:
  ipList: ""
  standbyIpList: ""
```

47

Edit the section to include the new auxiliary database station address as shown below:

Note: Security is always enabled. The auxDb secure flag is no longer required and if present may be removed.

Note: You must preserve the leading spaces in each line.

```
auxDb:
  ipList: "cluster_1_IP1,cluster_1_IP2 ... cluster_1_IPn"
  standbyIpList: "cluster_2_IP1,cluster_2_IP2 ... cluster_2_IPn"
```

where

cluster_1_IP1, *cluster_1_IP2*...*cluster_1_IPn* are the external IP addresses of the stations in the local cluster, including the new station address

cluster_2_IP1, *cluster_2_IP2*,*cluster_2_IPn* are the external IP addresses of the stations in the peer cluster, including the new station address; required only for geo-redundant deployment

48

Save and close the nsp-config.yml file.

49

Enter the following to put the changes into effect:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config --deploy

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

The NSP configuration is updated.

50

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↲
```

51

Enter the following:

```
# kubectl get pods -A ↲
```

The pods are listed.

52

Locate the auxiliary database agent pod entry, which resembles the following:

```
namespace     nspos-auxdb-agent-pod_ID     1/1     Running
0          uptime
```

53

Enter the following:

```
# kubectl delete pod nspos-auxdb-agent-pod_ID -n namespace ↲
```

where

namespace is the namespace of the pod entry in Step 52

pod_ID is the pod ID of the auxiliary database agent pod entry in Step 52

The pod is deleted and recreated to include the new station.

Start auxiliary database proxies

54

Perform the following step as the root user on one of the auxiliary database stations to enable and start the auxiliary database services:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh startAndEnableServices
↲
```

Note: For a geo-redundant auxiliary database, the step must be performed on a station in each auxiliary database cluster.

55

Close the open console windows.

END OF STEPS

20.15 How do I replace an auxiliary database station?

20.15.1 Purpose

Perform this procedure to replace an auxiliary database station with a station that has the same IP address, for example, after a hardware failure.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

To perform his procedure, the RHEL 9 OS must be installed on the auxiliary database station.

Note: Nokia recommends enabling password-free SSH between auxiliary database cluster hosts for the root user.

20.15.2 Steps

1

Add a hostname entry for the replacement station to the /etc/hosts file on each existing auxiliary database station.

Note: The hostname must be the fully qualified hostname, and not the short hostname.

Note: Hostnames are case-sensitive.

2

Log in as the root user on the replacement auxiliary database station.

3

Add a hostname entry to the /etc/hosts file on the replacement station using the following criteria.

- The first entry for the station hostname in the file must be the station IP address that is reachable by each main server and NSP cluster.
- The hostname must be the fully qualified hostname, and not the short hostname.
- The hostname must:
  - contain only ASCII alphanumeric and hyphen characters.
  - not begin or end with a hyphen.
  - not begin with a number.
  - comply with the format defined in IETF RFC 1034.
  - use period characters delimit the FQDN components.
  - not exceed 63 characters.

Note: Hostnames are case-sensitive.

4

Transfer the following auxiliary database installation files to an empty directory on the auxiliary database station:

Note: You must ensure that the directory is empty.

Note: In subsequent steps, the directory is called the software directory.

- nspos-auxdb-*R.r.p*-rel.*v*.rpm
- VerticaSw_PreInstall.sh
- nspos-jre-*R.r.p*-rel.*v*.rpm

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- vertica-*R.r.p*-rel.tar

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version number

5

Open a console window.

6

Navigate to the software directory.

Note: The directory must contain only the installation files.

7

Enter the following:

```
# chmod +x * ↵
```

8

Enter the following:

```
# ./VerticaSw_PreInstall.sh ↵
```

The script displays configuration messages like the following, and a prompt:

```
Logging Vertica pre install checks to log_file
INFO: About to set proxy parameters in /etc/profile.d/proxy.sh...
INFO: Completed setting proxy parameters in /etc/profile.d/proxy.sh...
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
conf...
INFO: Backing up /etc/logrotate.conf to /etc/logrotate.conf.orig
INFO: Removing /var/log/wtmp entry from /etc/logrotate.conf
INFO: Adding /etc/logrotate.d/wtmp
Checking user group nsp...
Adding user group nsp...
Checking user nsp...
Adding nsp...
Checking Linux user group samauxdb...
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Adding user group samauxdb...
Checking user samauxdb...
Adding samauxdb...
Set password for samauxdb... New password:
```

9

Enter a password that conforms to the RHEL password criteria.

The following prompt is displayed:

```
Retype new password:
```

10

Re-enter the password.

Messages like the following are displayed:

```
Changing password for user samauxdb.
passwd: all authentication tokens updated successfully.
Adding samauxdb to /etc/cron.allow
Moving logfile from /tmp ...
     ... to /opt/nsp/nfmp/auxdb/install/log
Changing ownership of the directory /opt/nsp/nfmp/auxdb/install to
samauxdb:samauxdb.
Removing group write and world permissions from the directory
/opt/nsp/nfmp/auxdb/install.
Appending Vertica section to /opt/nsp/nfmp/auxdb/install/.bashrc ...
Creating /opt/nsp/nfmp/auxdb/data for Vertica database files.
Changing ownership of /opt/nsp/nfmp/auxdb files.
INFO: Creating auxiliary database prep script.
INFO: Creating nspos-auxdb-prep systemd service.
INFO: Enabling nspos-auxdb-prep systemd service.

************************************************************************
* *
* Changes were made that require a restart. *
* Please restart this host before proceeding with Vertica
installation. *
* *
************************************************************************
```

11

Perform the following steps to restart the station.

1. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# systemctl reboot ↵
```

The station reboots.

2. When the reboot is complete, log in to the station as the root user.
3. Open a console window.
4. Navigate to the software directory.

12

Enter the following:

```
# tar xvf vertica-R.r.p-rel.tar $(tar tf vertica-R.r.p-rel.tar | sort
-V | tail -1) ↵
```

13

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/N]:
```

14

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

15

Log in to an existing auxiliary database station as the root user.

Note: The station must be an auxiliary database station other than the station that you are replacing.

16

Open a console window.

17

Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh prepRecoverNode
internal_IP ↵
```

where *internal_IP* is the internal auxiliary database IP address of the failed station

18

Reboot the new station.

1. Log in as the root user on the replacement station.
2. Enter the following to reboot the replacement station:

```
# systemctl reboot ↵
```

19

When the reboot of the station you are replacing is complete, enter the following on an existing auxiliary database station:

Note: The station must be an auxiliary database station other than the station that you are replacing.

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

20

Enter the following to recover the node:

```
# ./auxdbAdmin.sh recoverNode internal_IP ↵
```

where *internal_IP* is the internal auxiliary database IP address of the failed station

21

Enter the following on an existing auxiliary database station:

```
# ./auxdbAdmin.sh configureTLS ↵
```

22

Enter the following to restart the database proxies:

```
# ./auxdbAdmin.sh stopProxyService ↵
# ./auxdbAdmin.sh startProxyService ↵
```

23

Close the open console windows.

END OF STEPS

20.16 How do I remove an auxiliary database station?

20.16.1 Purpose

Perform this procedure to remove a station from an auxiliary database.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

CAUTION

Service Disruption

This procedure requires a restart of each main server, which is service-affecting.

Perform this procedure only during a scheduled maintenance period.

Note: If the auxiliary database is geo-redundant, the primary and standby clusters must have the same number of stations; if you remove a station from one cluster, you must also remove a station from the other cluster.

Note: *release-ID* in a file path has the following format:
R.r.p-rel.*version*
where
R.r.p is the NSP release, in the form *MAJOR.minor.patch*
version is a numeric value

20.16.2 Steps

1

If the auxiliary database is geo-redundant, you must identify which auxiliary database cluster is currently primary.

If you do not know which cluster is currently the primary cluster, perform 20.5 “How do I check the auxiliary database status?” (p. 527).

Remove station from standalone or primary cluster

2

Log in to one of the auxiliary database stations that is not being removed as the root user.

3

Open a console window.

4

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

5

Enter the following to stop and disable the auxiliary database services:

```
# ./auxdbAdmin.sh stopAndDisableServices ↵
```

Note: For a geo-redundant auxiliary database, the step must be performed on a station in each auxiliary database cluster.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Enter the following to stop the auxiliary database:

```
# ./auxdbAdmin.sh stop ↵
```

7

Enter the following to start the auxiliary database:

```
# ./auxdbAdmin.sh start ↵
```

8

Enter the following:

```
# ./auxdbAdmin.sh removeNode internal_IP ↵
```

where *internal_IP* is the IP address that the station uses to communicate with the other auxiliary database stations

You are prompted for the database user password.

9

Enter the password.

The removal operation begins.

Note: If a cluster rebalance is required, the operation may take considerable time, depending on the volume of data in the auxiliary database.
The station is removed from the auxiliary database.

10

If the NSP deployment does not include the NFM-P, or is geo-redundant, go to Step 12.

Reconfigure NFM-P, standalone auxiliary database

11

If the NSP deployment includes the NFM-P, perform the following steps on each NFM-P main server station.

Note: In a redundant NFM-P deployment, you must perform the steps on the standby main server station first.

1. Log in to the station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
bash$ ./nmsserver.bash appserver_status ↵
```

The server status is displayed; the server is fully stopped if the status is the following:

```
Application Server is stopped
```

If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

6. Enter the following to switch to the root user:

   ```
   bash$ su - ↵
   ```

7. Enter the following:

   ```
   # samconfig -m main ↵
   ```

8. Enter the following:

   ```
   <main> configure auxdb ip-list station_1_IP,station_2_IP,...
   station_n_IP exit ↵
   ```

   where

   station_1_IP,*station_2_IP*,...*station_n_IP* are the IP addresses of the remaining stations in the cluster

9. Enter the following:

   ```
   <main> apply ↵
   ```

   The configuration is applied.

10. Enter the following:

    ```
    <main> exit ↵
    ```

    The samconfig utility closes.

11. Enter the following to switch back to the nsp user:

    ```
    # exit ↵
    ```

Reconfigure auxiliary database cluster

12

Log in as the root user on one of the remaining auxiliary database stations in the cluster.

13

Open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14



CAUTION

Service disruption

Changing a parameter in the auxiliary database install.config file can have serious consequences that include service disruption.

Do not change any parameter in the install.config file, other than the parameters described in the steps, without guidance from technical support.

Locate the following line and delete the IP address of the station that is being removed:

hosts=*internal_IP1*,*internal_IP2*...*internal_IPn*

15

Locate the following line and delete the IP address entries of the station that is being removed:

export_hosts=*internal_IP1*[*export_IP1*],*internal_IP2*[*export_IP2*]...*internal_IPn*[*export_IPn*]

16

Save and close the install.config file.

17

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

18

Enter the following:

```
# ./auxdbAdmin.sh distributeConfig ↵
```

The updated configuration is distributed to the other auxiliary database stations in the cluster.

19

Enter the following to start and enable the auxiliary database services:

```
# ./auxdbAdmin.sh startAndEnableServices ↵
```

20

If the auxiliary database is standalone, go to Step 28.

Configure standby cluster

21

Log in as the root user on the station that is to be removed from the standby auxiliary database cluster.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The station that you remove from the standby cluster must be the station that occupies the same list position in the NFM-P main server configuration. For example, if the stations in the primary cluster are listed in the order 1, 2, 3, and you are removing station 2, you must remove the second station listed in the configuration of the standby cluster.

22

Enter the following:

```
# /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh removeNode internal_IP
↵
```

where *internal_IP* is the IP address that the station uses to communicate with the other auxiliary database stations in the cluster

You are prompted for the database user password.

23

Enter the password.

The operation begins.

Note: If a cluster rebalance is required, the operation may take considerable time, depending on the volume of data in the auxiliary database.
The station is removed from the auxiliary database.

24

Log in as the root user on one of the remaining auxiliary database stations in the standby cluster.

25

Enter the following:

```
# cd /opt/nsp/nfmp/auxdb/install/bin ↵
```

26

Perform Step 13 to Step 19.

27

If the NSP deployment does not include the NFM-P, go to Step 29.

Reconfigure NFM-P, geo-redundant auxiliary database

28

Perform the following steps on each main server in each data center.

Note: In a redundant NFM-P deployment, you must perform the steps on the standby main server first.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

5. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.
6. Enter the following to switch to the root user:

   ```
   bash$ su - ↲
   ```

7. Enter the following:

   ```
   # samconfig -m main ↲
   ```

8. Enter the following:

   Note: The order of the IP addresses must be the same on each main server in the geo-redundant system.

   ```
   <main> configure auxdb ip-list IP_list exit ↲
   ```

   where

   IP_list is a list of the IP addresses in the following format:

   cluster_1_IP1,*cluster_1_IP2*,*cluster_1_IPn*;*cluster_2_IP1*,*cluster_2_IP2*,*cluster_2_IPn*
9. Enter the following:

   ```
   <main> apply ↲
   ```

   The configuration is applied.
10. Enter the following:

    ```
    <main> exit ↲
    ```

    The samconfig utility closes.
11. Enter the following to switch back to the nsp user:

    ```
    # exit ↲
    ```

Configure NSP clusters

29

Perform Step 31 to Step 37 on the NSP cluster in each data center.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

30

Go to Step 38.

31

Log in as the root or NSP admin user on the NSP deployer VM.

32

Open the following file using a plain-text editor such as vi:

/opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

33

Locate the following section:

```
auxDb:
  ipList: "cluster_1_IP1,cluster_1_IP2...cluster_1_IPn"
  standbyIpList: "cluster_2_IP1,cluster_2_IP2...cluster_2_IPn"
```

34

Delete the IP address of each auxiliary database station that you are removing.

35

Save and close the file.

36

Enter the following to start the NSP cluster:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the nspdeployerctl command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --config --deploy

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config
--deploy ↵
```

The NSP cluster starts, and the configuration update is put into effect.

37

Close the console window.

Start NFM-P main servers

38

If the NSP deployment includes the NFM-P, start each main server.

Note: In a DR deployment, you must start the primary main server first.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

1. Log in to the station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↲
   ```

The main server starts.

39

Close the open console windows.

END OF STEPS

20.17 How do I recreate an auxiliary database?

20.17.1 Purpose

If an NSP auxiliary database is not functioning and cannot return to operational status, you may need to recreate the database. Depending on the severity of the failure, however, Nokia support may be able to repair the database.

Perform this procedure only if all attempts to repair the auxiliary database fail, there is no database backup from which the database may be restored, and Nokia support directs you to recreate the database.

Note: If you are performing this procedure to recover from a failed upgrade, uninstall and install the auxiliary database, then restore the backup taken prior to upgrade as described in the *NSP Installation and Upgrade Guide* instead of executing this procedure.

20.17.2 Steps

1

If possible, back up the auxiliary database to preserve it for potential data recovery. If data recovery is not required, you can skip this step.

Note: The auxiliary database must be running in order for a backup to be successful. If the auxiliary database cannot be started, you cannot create a database backup.

2

In order to back up an auxiliary database, all members of the local auxiliary database cluster must be operational and available, or the backup fails. Perform 20.5 “How do I check the auxiliary database status?” (p. 527) to verify that each local cluster member is operational.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Perform the following steps on each auxiliary database station to collect the auxiliary database log files.

Note: You cannot specify /tmp, or any directory below /tmp, as the output directory.

1. Log in to the station as the root user.
2. Enter the following:

   # /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles *output_dir days* ↵

   where

   output_dir is a local directory that is to contain the output files

   days is the optional number of days for which to collect log files; if not specified, all logs are collected

4

On one auxiliary database station, open the /opt/nsp/nfmp/auxdb/install/config/install.config file using a plain-text editor such as vi.

5

Ensure that the internal and external IP addresses in the following lines are correctly assigned to the auxiliary database stations:

```
hosts=internal_IP1,internal_IP2...internal_IPn
export_hosts=internal_IP1[export_IP1],internal_IP2[export_IP2]...
internal_IPn[export_IPn]
```

6

If you intend to reuse existing auxiliary database stations, uninstall the auxiliary database as described in the *NSP Installation and Upgrade Guide*.

7

Install the auxiliary database as described in the *NSP Installation and Upgrade Guide*.

Note: When prompted to enter passwords for auxiliary database users, you must use the same passwords that were previously used for each user.

Reconfigure NFM-P auxiliary database tables

8

If the NSP deployment does not include the NFM-P, go to Step 15.

9

When the auxiliary database is fully initialized, perform the following steps on each NFM-P main server station to start the main server, if the server is not started.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: In a redundant system, you must start the primary main server first.

1. Log in as the root user on the main server station.
2. Open a console window.
3. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↲
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

The main server detects the auxiliary database reinstallation, raises a Critical alarm against the auxiliary database, and begins recreating the auxiliary database schema.

Note: If the main server fails to recreate the schema, the server retries periodically until all schema elements are created.

When the schema recreation is complete, the reinstallation alarm clears, and the NFM-P raises a Major alarm that you must clear manually.

10

If the auxiliary database includes custom data tables, perform the following steps to recreate and repopulate the tables.

1. Log on to the standalone or primary main server station as the nsp user.
2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

3. Create each custom table, as described in Step 6 of 20.19 “How do I create and manage custom auxiliary database table attributes in NFM-P?” (p. 583), using the saved XML file that defines the table.
4. Add the required data to each table, as described in Step 7 of 20.19 “How do I create and manage custom auxiliary database table attributes in NFM-P?” (p. 583), using the saved CSV file for the table.

11

If you use the Analytics dynamic inventory reporting function, you must recreate the custom inventory tables and dynamic Analytics managed-object definitions.

1. Remove the existing dynamic Analytics managed-object definitions; enter the following on the main server station:

   ```
   bash$ ./nmsserver.bash dynamic_analyticmo remove class mo_name ↲
   ```

   where

   class is the object class

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

mo_name is the name of the dynamic Analytics managed object

2. Create the custom inventory tables; enter the following:

   ```
   bash$ ./customData.bash --createTables XML_file ↲
   ```

   where *XML_file* is the saved XML file that defines the custom inventory tables

3. Create the dynamic Analytics managed-object definitions; enter the following:

   ```
   bash$ ./nmsserver.bash dynamic_analyticmo create dyn_inv_XML_file ↲
   ```

   where *dyn_inv_XML_file is* the absolute path and name of the saved XML file that defines the Analytics dynamic inventory configuration

12

If you have created dynamic aggregations, recreate the aggregations.

Note: Any previous aggregation data is lost during the auxiliary database schema recreation earlier in the procedure.

1. Enter the following on the main server station for each dynamic aggregation to remove the aggregation:

   ```
   bash$ ./nmsserver.bash dynamic_aggregation remove aggregation ↲
   ```

   where *aggregation* is the name of the aggregation

2. Enter the following to create the dynamic aggregation:

   ```
   bash$ ./nmsserver.bash dynamic_aggregation create agg_XML_file ↲
   ```

   where *agg_XML_file is* the absolute path and name of the saved XML file that defines the aggregation configuration

3. Re-enable the dynamic aggregations using an NFM-P XML API or GUI client.

13

If you use periodic accounting tables, enter the following on the main server station to create the tables:

Note: Any previous periodic accounting data is lost during the auxiliary database schema recreation earlier in the procedure.

```
bash$ ./nmsserver.bash accountingPeriodic create per_acc_XML_file ↲
```

where *per_acc_XML_file is* the absolute path and name of the saved XML file that defines the periodic accounting configuration

14

Close the open console windows.

Reset the collection schema

15

Log in as the root or NSP admin user on the NSP deployer host.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

16

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/mdm/bin ↵
# ./yang-files.bash --user user --pass password --reset collection ↵
```

Undeploy the NSP

17

Log in as the root or NSP admin user on the NSP deployer host.

18

Perform Step 19 to Step 22 on each NSP cluster, and then go to Step 24.

Note: In a DR deployment, you must perform the steps first on the standby cluster.

19

Perform the following steps to preserve the existing deployment configuration.

1. Open the following file using a plain-text editor such as vi:

   /opt/nsp/NSP-CN-DEP-*release-ID*/NSP-CN-*release-ID*/config/nsp-config.yml

2. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

   ```
   deleteOnUndeploy:false
   ```

3. Save and close the file.

20

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

21

Enter the following to undeploy the NSP:

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass uninstall --undeploy

```
# ./nspdeployerctl uninstall --undeploy ↵
```

22

On the NSP deployer host, enter the following:

```
# export KUBECONFIG=/opt/nsp/nsp-configurator/kubeconfig/nsp_
kubeconfig ↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

23

Enter the following periodically to display the status of the Kubernetes system pods:

Note: You must not proceed to the next step until the output lists only the following:

- pods in kube-system namespace
- nsp-backup-storage pod

```
# kubectl get pods -A ↵
```

The pods are listed.

Redeploy the NSP

24

Enter the following to redeploy the NSP:

Note: In a DR deployment, you must perform the steps first on the primary cluster.

Note: If the NSP cluster VMs do not have the required SSH key, you must include the --ask-pass argument in the command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:
nspdeployerctl --ask-pass install --deploy

```
# ./nspdeployerctl install --deploy ↵
```

The re-creation of the auxiliary database collection tables begins.

Do not perform the next step until the auxiliary database collection tables are fully initialized.

25

Close the open console windows.

Reconfigure NSP auxiliary database tables

26

If auxiliary database custom data tables were present before the reinstallation, reconfigure the custom data tables as described in procedure: 20.20 “How do I create and manage custom auxiliary database table attributes in NSP?” (p. 585).

27

If auxiliary database anonymization was enabled before the reinstallation, re-enable anonymization for Analytics reports as described in the *NSP Analytics Report Catalog*.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.18 How do I customize auxiliary database tables?

20.18.1 Custom auxiliary database table attributes

Some NSP Analytics reports require data that is not available by default. Data such as location names, geographic co-ordinates, and maintenance windows must be imported to an auxiliary database in order to be included in reports. The NSP and NFM-P have a mechanism for the creation and management of auxiliary database tables and content.

An XML file that you create defines the table columns and data types to add to an auxiliary database. After you import a table definition to the NSP or NFM-P, an operator can add data records to the table using a CSV file whose record format matches the format defined in the XML file. An operator can also delete one or more tables, or the content of a table.

Note: A data-import operation appends the new records to the table, and does not affect the existing table contents or structure.

Custom auxiliary database table attributes are retained through system upgrades, and are included in auxiliary database backup and restore operations.

Table definition file format

Figure 20-1, “Custom table definition file format” (p. 579), shows a table definition XML file that contains the column definitions for two custom tables.

Figure 20-1 Custom table definition file format

```
<customTablesConfig organization="OurCompany" name="CustomTableDefs"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:noNamespaceSchemaLocation="./schema/customtables.xsd">
   <customTables>
      <customTable
         name="table1"
         description="This is table 1"
         orderBy="column1">
         <columns>
            <column name="column1" type="STRING" length="8" encoding="RLE" />
            <column name="column2" type="INTEGER" />
            <column name="column3" type="FLOAT" />
            <column name="column4" type="BOOLEAN" />
            <column name="column5" type="NUMERIC" precision="12" scale="4" />
         </columns>
      </customTable>
      <customTable
         name="table2"
         description="This is table 2"
         segmentedBy="column1,column2">
         <columns>
            <column name="column1" type="STRING" length="64" />
            <column name="column2" type="STRING" length="64" />
         </columns>
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
      </customTable>
   </customTables>
</customTablesConfig>
```

Table 20-1, “Custom attribute definition elements” (p. 580) lists and describes the configurable elements in a custom table definition.

Table 20-1 Custom attribute definition elements

Element	Description
description	Text that describes the table; optional
orderBy	Comma-separated list of column names that define how the table data is to be ordered; optional
segmentedBy	Comma-separated list of column names that define how the table is to be segmented; optional
column name	Table column name
type	One of the following: • STRING—1 to 4096 characters • INTEGER • FLOAT • BOOLEAN • NUMERIC
precision	Maximum number of significant digits, represented by a positive integer less than or equal to 1024; required for NUMERIC data type
scale	Maximum number of digits to the right of the decimal point in a NUMERIC data type, represented by a positive integer less than or equal to the precision value; if omitted, defaults to 0 If the number of decimal digits in a data value exceeds the scale value, the data value is rounded to the number of digits specified by the scale value.
encoding	Text encoding type for STRING data type; optional, default is AUTO
length	Field length; required for STRING data type

Functional description

For NFM-P, the management tool for custom tables is the customData.bash CLI script on a main server station.

For NSP, the management tool for custom tables is the customdata.bash CLI script on an active auxiliary database station.

You can use the tool to do the following:

- create and delete tables
- import, export, and delete data

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- list the currently defined custom tables
- export a table schema

Note: In order for the customData.bash script to function on NFM-P, the main server configuration must include an auxiliary database.

Note: In order to run the customdata.bash script on NSP, the NSP deployment must include an auxiliary database, and NSP is started so that NSP can create auxiliary database users.

Note: If a string data value to be imported includes a comma, you must precede the comma with a backslash to prevent the comma from being interpreted as a CSV file delimiter.

The customData.bash script and customdata.bash script have the following operating characteristics:

- The script automatically assigns a prefix and suffix to the name of a custom table.
  - For NFM-P, references to the table in script operations after table creation must include the samdb prefix and _ct suffix; for example, customTable1 must be specified as samdb.customTable1_ct.
  - For NSP, references to the table in script operations after table creation must include the custom_data prefix and _ct suffix; for example, customTable1 must be specified as custom_data.customTable1_ct.
- For NFM-P, script operations that modify data, such as createTable, deleteTable, and importData, require the auxiliary database user password.
- For NSP, all script operations require the auxiliary database user password.
- During a createTable operation, a formatting error in a table definition causes all table creation during the operation to fail, and the script saves the table definition file as tmp/customtables.xml.template.
- For NFM-P, the script logs each operation in the /opt/nsp/nfmp/server/nms/log/customdata.log; the maximum log size is five Mbytes.
- For NSP, the script logs each operation in the /opt/nsp/nfmp/auxdb/install/custom-data/logs/ directory; the log file format is custom-data-yyyy.MM.dd-HH.mm.ss.log. A new log is produced each time the customdata.bash script is run.

Static custom data tables in NSP

Static custom data table definitions are included in NFM-P, which creates and upgrades these tables automatically.

If you want to use static custom data tables in NSP, you must install the static custom data table definitions. The NSP custom data tool includes these definitions in the /opt/nsp/nfmp/auxdb/install/custom-data/table-definitions/predefined/ directory:

- anl_details.xml
- maintenance_window.xml

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

20.19 How do I create and manage custom auxiliary database table attributes in NFM-P?

20.19.1 Purpose

Use this procedure to do the following in NFM-P:

- Add data to a custom table
- Create a custom table
- Delete a custom table or data in a custom table
- Export data or custom table schema to a file
- Import date to custom table
- List all custom tables

Note: The *password* value that you specify in the following steps is the password of the samauxdb user.

20.19.2 Steps

1

If you are creating a custom table, configure the elements in a table definition XML file using the format described in "Table definition file format" (p. 580), and store the file securely in a remote location.

2

If you are adding data to a custom table, create a CSV-formatted data file that has the same record format as the custom table, and store the file securely in a remote location.

3

Log in to the standalone or primary main server station as the nsp user.

4

Open a console window.

5

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

6

To create a custom table, enter the following:

```
bash$ ./customData.bash -password password -createTables definition_file ↵
```

where *definition_file* is the table definition XML file created in Step 1

The specified tables are created.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

To import data to a custom table, enter the following:

```
bash$ ./customData.bash -password password -importData table_name
data_file ↲
```

where

data_file is the CSV data file created in Step 2

table_name is the table to which the data is to be imported

The data is imported.

8

To list all custom tables, enter the following:

```
bash$ ./customData.bash -listTables ↲
```

The tables are listed.

9

To delete all data in a custom table, enter the following:

```
bash$ ./customData.bash -password password -deleteData samdb.table_ct
↲
```

where *table* is the name of the table from which to delete data

The table data is deleted.

10

To delete a custom table, enter the following:

```
bash$ ./customData.bash -password password -deleteTable samdb.table_ct
↲
```

where *table* is the name of the table to delete

The table is deleted.

11

To export the data in a custom table to a file, enter the following:

```
bash$ ./customData.bash -exportData samdb.table_ct output_file ↲
```

where

table is the name of the table from which to export data

output_file is the name of the file that is to contain the exported data

The table data are exported to the file.

12

To export a custom table schema to a file, enter the following:

```
bash$ ./customData.bash -tableSchema samdb.table_ct output_file ↲
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

where

table is the name of the table from which to export the schema

output_file is the name of the file that is to contain the exported schema

The table schema is saved in the file.

13

Close the console window.

END OF STEPS

20.20 How do I create and manage custom auxiliary database table attributes in NSP?

20.20.1 Purpose

Use this procedure to do the following in NSP:

- Add data to a custom table
- Create a custom table
- Delete a custom table or data in a custom table
- Export data or custom table schema to a file
- Import date to custom table
- Install a static custom data table
- List all custom tables

Note: The *password* value that you specify in the following steps is the password of the samauxdb auxiliary database user.

20.20.2 Steps

1

If you are creating a custom table, configure the elements in a table definition XML file using the format described in “Table definition file format” (p. 580), and store the file securely in a remote location.

2

If you are adding data to a custom table, create a CSV-formatted data file that has the same record format as the custom table, and store the file securely in a remote location.

3

Log in as the root user on an auxiliary database station on an active auxiliary database cluster.

4

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Navigate to the /opt/nsp/nfmp/auxdb/install/custom-data/bin directory.

6

To create a custom table, enter the following:

```
bash$ ./customdata.bash -password password -createTables definition_file ↲
```

where *definition_file* is the table definition XML file created in Step 1

The specified tables are created.

7

If you want to install the static custom data table definitions, enter the following:

```
bash$ ./customdata.bash -password password -createTables definition_file ↲
```

where *definition_file* is a predefined static table definition XML file listed in "Static custom data tables in NSP" (p. 582)

The specified tables are created.

8

To import data to a custom table, enter the following:

```
bash$ ./customdata.bash -password password -importData table_name data_file ↲
```

where

data_file is the CSV data file created in Step 2

table_name is the table to which the data is to be imported

The data is imported.

9

To list all custom tables, enter the following:

```
bash$ ./customdata.bash -listTables ↲
```

The tables are listed.

10

To delete all data in a custom table, enter the following:

```
bash$ ./customdata.bash -password password -deleteData custom_data.table_ct ↲
```

where *table* is the name of the table from which to delete data

The table data is deleted.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

To delete a custom table, enter the following:

```
bash$ ./customdata.bash -password password -deleteTable custom_data.table_ct ↵
```

where *table* is the name of the table to delete

The table is deleted.

12

To export the data in a custom table to a file, enter the following:

```
bash$ ./customdata.bash -exportData custom_data.table_ct output_file ↵
```

where

table is the name of the table from which to export data

output_file is the name of the file that is to contain the exported data

The table data are exported to the file.

13

To export a custom table schema to a file, enter the following:

```
bash$ ./customdata.bash -tableSchema custom_data.table_ct output_file ↵
```

where

table is the name of the table from which to export the schema

output_file is the name of the file that is to contain the exported schema

The table schema is saved in the file.

14

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21 Classic management administration

NFM-P component administration

21.1 Pathway: redundant NFM-P shutdown and restart

21.1.1 Description

The following is the sequence of high-level actions required to stop and start the redundant NFM-P system components in a graceful manner for maintenance purposes.

21.1.2 Stages

Align redundancy roles

1

If the primary main server and database are in separate data centers, perform 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) to align the primary components in the primary data center.

Perform orderly shutdown of standby components

2

If the system includes an auxiliary database, stop the auxiliary database cluster in the standby data center, as described in 20.4 “How do I stop an auxiliary database cluster?” (p. 525).

3

If the system includes one or more auxiliary servers, perform the following steps; see 21.7 “How do I stop an auxiliary server?” (p. 597) for information.

1. Stop each Reserved auxiliary server of the standby main server.
2. Stop each Preferred auxiliary server of the standby main server.

4

Stop the standby main server, as described in 21.3 “How do I stop a main server?” (p. 593).

5

Stop the standby main database.

1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```

4. Enter the following to stop the main database:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# systemctl stop nfmp-main-db.service ↵
```

Perform maintenance on standby components

6

Perform the required maintenance on the NFM-P components in the standby data center.

Perform orderly startup of standby components

7

Start the standby main database.

1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to start the Oracle proxy:

   ```
   # systemctl start nfmp-oracle-proxy.service ↵
   ```

4. Enter the following to start the main database:

   ```
   # systemctl start nfmp-main-db.service ↵
   ```

8

Start the standby main server, as described in 21.2 “How do I start a main server?” (p. 593).

9

If the system includes one or more auxiliary servers, perform the following steps; see 21.6 “How do I start an auxiliary server?” (p. 596) for information.

1. Start each Reserved auxiliary server of the standby main server.
2. Start each Preferred auxiliary server of the standby main server.

10

If the system includes one or more auxiliary servers, perform the following steps; see 21.6 “How do I start an auxiliary server?” (p. 596) for information.

1. Start each Preferred NFM-P auxiliary server of the standby main server.
2. Start each Reserved NFM-P auxiliary server of the standby main server.

11

If the system includes an auxiliary database, start the auxiliary database cluster in the standby data center, as described in 20.3 “How do I start an auxiliary database cluster?” (p. 523).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Switch redundancy roles

12

Perform a server activity switch to change the standby main server role to primary, as described in 16.11 “How do I perform a server activity switch?” (p. 484).

The standby main server assumes the primary role.

13

If automatic database realignment is not enabled, perform a database switchover; perform 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) or 16.14 “How do I perform a main database switchover using a CLI script?” (p. 487).

The standby main database assumes the primary role.

Perform orderly shutdown of former primary components

14

If the system includes an auxiliary database, stop the auxiliary database cluster in the former primary data center, as described in 20.4 “How do I stop an auxiliary database cluster?” (p. 525).

15

If the system includes one or more auxiliary servers, perform the following steps; see 21.7 “How do I stop an auxiliary server?” (p. 597) for information.

1. Stop each Reserved auxiliary server of the former primary main server.
2. Stop each Preferred auxiliary server of the former primary main server.

16

Stop the former primary main server, as described in 21.3 “How do I stop a main server?” (p. 593).

17

Stop the former primary main database.

1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```

4. Enter the following to stop the main database:

   ```
   # systemctl stop nfmp-main-db.service ↵
   ```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Perform maintenance on former primary components

18

Perform the required maintenance on the NFM-P components in the former primary data center.

Perform orderly startup of former primary components

19

Start the former primary main database.

1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to start the Oracle proxy:

   # **systemctl start nfmp-oracle-proxy.service** ↵
4. Enter the following to start the main database:

   # **systemctl start nfmp-main-db.service** ↵

20

Start the former primary main server, as described in 21.2 “How do I start a main server?” (p. 593).

21

If the system includes one or more auxiliary servers, perform the following steps; see 21.6 “How do I start an auxiliary server?” (p. 596) for information.

1. Start each Reserved auxiliary server of the former primary main server.
2. Start each Preferred auxiliary server of the former primary main server.

22

If the system includes one or more auxiliary servers, perform the following steps; see 21.6 “How do I start an auxiliary server?” (p. 596) for information.

1. Start each Preferred NFM-P auxiliary server of the former primary main server.
2. Start each Reserved NFM-P auxiliary server of the former primary main server.

23

If the system includes an auxiliary database, start the auxiliary database cluster in the former primary data center, as described in 20.3 “How do I start an auxiliary database cluster?” (p. 523).

Restore initial redundancy roles

24

If required, restore the initial redundancy roles so that the former primary main server and

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

database again assume the primary roles.

1. Perform a server activity switch to restore the initial primary and standby main server roles, as described in 16.11 “How do I perform a server activity switch?” (p. 484).

   The former primary and standby main server roles are restored.

25

If automatic database realignment is not enabled, perform a database switchover; perform 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) or 16.14 “How do I perform a main database switchover using a CLI script?” (p. 487).

The former primary and standby main database roles are restored.

21.2 How do I start a main server?

21.2.1 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash start ↵
```

The main server starts.

4

Close the console window.

END OF STEPS

21.3 How do I stop a main server?



CAUTION

Service Disruption

Performing this procedure may be service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.3.1 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Enter the following:

```
bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
```

4

Enter the following:

```
bash$ ./nmsserver.bash stop ↲
```

5

Enter the following:

```
bash$ ./nmsserver.bash appserver_status ↲
```

The server status is displayed; the server is fully stopped if the status is the following:

```
Application Server is stopped
```

If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

6

Enter the following to switch to the root user:

```
bash$ su - ↲
```

END OF STEPS

21.4 How do I start a main database?



CAUTION

Service Disruption

Performing this procedure may be service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.4.1 Steps

1

Log in to the main database station as the root user.

2

Open a console window.

3

Enter the following to start the Oracle proxy:

```
# systemctl start nfmp-oracle-proxy.service ↵
```

4

Enter the following to start the main database:

```
# systemctl start nfmp-main-db.service ↵
```

5

Close the console window.

END OF STEPS

21.5 How do I stop a main database?



CAUTION

Service Disruption

Performing this procedure may be service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.

21.5.1 Steps

1

Log in to the main database station as the root user.

2

Open a console window.

3

Enter the following to stop the Oracle proxy:

```
# systemctl stop nfmp-oracle-proxy.service ↵
```

4

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Enter the following to stop the main database:

```
# systemctl stop nfmp-main-db.service ↵
```

5

Close the console window.

END OF STEPS

21.6 How do I start an auxiliary server?

21.6.1 Steps

1

Choose Administration→System Information from the NFM-P main menu. The System Information form opens.

2

Click on the Auxiliary Servers tab.

3

Select the auxiliary server and click Properties. The Auxiliary Server (Edit) form opens.

4

Set the Operation Mode parameter to In Service.

5

Click OK to commit the change and close the form.

6

Close the System Information form.

7

Log in to the auxiliary server station as the nsp user.

8

Open a console window.

9

Enter the following:

```
bash$ /opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxstart ↵
```

The auxiliary server starts.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

10

Close the console window.

END OF STEPS

21.7 How do I stop an auxiliary server?



CAUTION

Service Disruption

Performing this procedure may be service-affecting.

Ensure that you perform this procedure only during a scheduled maintenance period.

21.7.1 Steps

1

Choose Administration→System Information from the NFM-P main menu. The System Information form opens.

2

Click on the Auxiliary Servers tab.

3

Select the auxiliary server and click Properties. The Auxiliary Server (Edit) form opens.

4

Set the Operation Mode parameter to In Maintenance Mode.

5

Click OK to commit the change and close the form.

The auxiliary server stops.

6

Close the System Information form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P administration and management

21.8 What is global NFM-P system configuration?

21.8.1 Introduction

The NFM-P may require a configuration change to meet specific operational requirements. You can use the procedures in this section to configure global NFM-P settings, functions, and preferences.

Graceful NFM-P system shutdown and startup



CAUTION

Service Outage

Stopping the NFM-P software on a station, or rebooting a station that hosts NFM-P software, may have serious consequences that can include a complete network management outage.

You must perform such service-affecting actions only as directed by the NSP documentation or technical support, and only during a scheduled maintenance period.

Low-level maintenance that is not described in this section, for example, applying a RHEL OS patch to the NFM-P component stations, may require that you stop and start each station.

Stopping a standalone NFM-P system creates a network management outage that must be considered in the planning for a maintenance activity that requires such action.

In a redundant NFM-P system, you can avoid such an outage by performing the orderly shutdown and startup of the components described in 21.1 “Pathway: redundant NFM-P shutdown and restart” (p. 589).

Global GUI-client updates

The NFM-P auto-client update function allows you to reconfigure multiple GUI clients using one central configuration. See the *NSP Installation and Upgrade Guide* for client update configuration information, and 21.14 “How do I modify the base configuration of all GUI clients?” (p. 612) for information about using the auto-update function to push an update to all GUI clients.

21.9 How do I change default text-field and ID ranges?

21.9.1 Format and range policies overview

You can use NFM-P format policies and range policies to change the default number and format of characters used for text fields, and the ID ranges used for managed objects.

21.9.2 Format and range policies

Format policies manage how services, policies, LSPs, and L2 and L3 access interfaces are named and described. Range policies manage the ID values that are assigned to services, policies, LSPs, and L2 and L3 access interfaces. For example, you can configure the following:

- a range policy that specifies a range of 200 to 499 for service IDs

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- a format policy that specifies a 15-character limit for service names

The object creation form indicates when a range or format policy is in effect for an object.

Format and range policies are not distributed to NEs. The format and range policies apply only to GUI creation of services, policies, LSPs, and L2 and L3 access interfaces. You cannot configure format and range policies when the services, LSPs, and L2 and L3 access interfaces are created using templates. However, the NFM-P allows an operator to use preconfigured examples of LSPs and services that have format and range policies applied to them. You can use the examples to create templates.

See 21.12 “How do I create or configure a format policy?” (p. 608) for information about configuring a format policy.

See 21.13 “How do I create or configure a range policy?” (p. 610) for information about configuring a range policy.

The following table lists the objects and associated parameters that can be managed using format and range policies.

Table 21-1 Format and Range policy objects and associated parameters

Object name	Format policy parameter	Range policy parameter
B-VPLS Service Site	Description, Name	—
Bypass-only LSP	Description, Name	ID
Customer	—	ID
Dynamic LSP	Description, Name	ID
I-VPLS Service Site	Description, Name	—
IES Group Interface	Description, Name	Interface ID
IES L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value
IES Service	Description, Service Name	Service ID
IES Service Access Point	Description, Name	Outer Encapsulation Value
IES Service Site	Description, Name	—
IES Subscriber Interface	Description, Name	Interface ID
IP Mirror Interface	—	Interface ID
MVPLS B-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS I-L2 Access Interface	Description	Outer Encapsulation Value
MVPLS L2 Access Interface	Description	Outer Encapsulation Value
MVPLS Service	Description, Service Name	Service ID
Mirror L2 Access Interface	—	Outer Encapsulation Value
MVPLS Service B-Site	Description, Name	—
MVPLS Service I-Site	Description, Name	—

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-1 Format and Range policy objects and associated parameters (continued)

Object name	Format policy parameter	Range policy parameter
MVPLS Service Site	Description, Name	—
Mirror Service	Description, Service Name	Service ID
Mirror Service Site	Description, Name	—
Redundant Interface	—	Interface ID
Spoke SDP Binding	—	VC ID
Static LSP	Description, Name	ID
Tunnel	Description, Name	ID
VLAN L2 Access Interface	Description	—
VLAN Service	Description, Service Name	Service ID
VLAN Service Access Point	Description, Name	—
VLAN Service Site	Description, Name	—
VLL Apipe Service	Description, Service Name	Service ID
VLL Apipe Service Site	Description, Name	—
VLL Cpipe Service	Description, Service Name	Service ID
VLL Cpipe Site	Description, Name	—
VLL Epipe Service	Description, Service Name	Service ID
VLL Epipe Service Site	Description, Name	—
VLL Fpipe Service	Description, Service Name	Service ID
VLL Fpipe Service Site	Description, Name	—
VLL Ipipe L2 Access Interface	Description	Outer Encapsulation Value
VLL Ipipe Service	Description	Service ID
VLL Ipipe Site	Description, Name	—
VLL L2 Access Interface	Description	Outer Encapsulation Value
VPLS B-L2 Access Interface	Description	Outer Encapsulation Value
VPLS I-L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Access Interface	Description	Outer Encapsulation Value
VPLS L2 Management Interface	—	Interface ID
VPLS Service	Description, Service Name	Service ID
VPLS Service Site	Description, Name	—
VPRN Group Interface	Description, Name	Interface ID
VPRN L3 Access Interface	Description, Name	Interface ID, Outer Encapsulation Value

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-1 Format and Range policy objects and associated parameters (continued)

Object name	Format policy parameter	Range policy parameter
VPRN Service	Description, Service Name	Service ID
VPRN Service Access Point	Description, Name	Outer Encapsulation Value
VPRN Service Site	Description, Name	—
VPRN Subscriber Interface	Description, Name	Interface ID

The following table lists the policies that support format and range policies.

Table 21-2 Format and Range policy objects and associated parameters for policies

Policy	Format policy	Range policy
Access Ingress QoS	Description, Displayed Name	ID
Access Egress QoS	Description, Displayed Name	ID
ATM QoS policy	Description, Displayed Name	ID
Egress Queue Group template	Description, Displayed Name	—
7705 SAR Fabric Profile	Description, Displayed Name	ID
Policer Control policy	Description, Displayed Name	—
HSMDA Pool policy	Description, Displayed Name	—
HSMDA Scheduler policy	Description, Displayed Name	—
HSMDA WRED Slope policy	Description, Displayed Name	—
Ingress Queue Group template	Description, Displayed Name	—
MCFR Egress QoS Profile	Description	Profile ID
MCFR Ingress QoS Profile	Description	Profile ID
MLPPP Egress QoS Profile	Description	Profile ID
MLPPP Ingress QoS Profile	Description	Profile ID
Named Buffer Pool policy	Description, Name	—
Network policy	Description, Displayed Name	ID
Network Queue	Description, Name	—
Port Scheduler policy	Description, Displayed Name	—
Sap Access Ingress for 7210	Description, Displayed Name	ID
Network Policy for 7210	Description, Displayed Name	NW Mgr ID, Policy Id
Network Queue for 7210	Description, Name	—
Port Access Egress for 7210	Description, Displayed Name	ID
Port Scheduler for 7210	Description, Displayed Name	—
Slope Policy for 7210	Description, Displayed Name	—

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-2 Format and Range policy objects and associated parameters for policies (continued)

Policy	Format policy	Range policy
Scheduler policy	Description, Displayed Name	—
WRED Slope policy	Description, Displayed Name	—
ACL IP filter	Description, Displayed Name	Filter ID
ACL IPv6 filter	Description, Displayed Name	Filter ID
ACL MAC filter	Description, Displayed Name	Filter ID
ANCP policy	Displayed Name	—
Host Tracking policy	Description, Displayed Name	—
MSAP policy	Description, Displayed Name	—
PPPoE policy	Description, Displayed Name	—
SLA Profile	Description, Displayed Name	—
Subscriber Explicit Map Entry	Description, Displayed Name	—
Subscriber Identification policy	Description, Displayed Name	—
Subscriber Profile	Description, Displayed Name	—
Egress Multicast Group	Description, Displayed Name	—
Multicast Package	Description, Displayed Name	ID
Multicast CAC	Description, Name	—
Multicast PathMgmt BW policy	Description, Name	—
Multicast PathMgmt Info policy	Description, Name	—
AS Path	Description, AS Path Name	—
Community	Description, Community Name	—
Community Member	Community Member	—
Damping	Damping Name	—
Prefix List	Description, Prefix List Name	—
Statement	Description, Statement Name	—
Service L3 Routing	Export Target IP Address, Import Target IP Address, Target IP Address	Export Target AS Value, Export Target AS Value (4Byte), Export Target Community Value, Export Target Extended Community Value, Export Target AS Value, Import Target AS Value (4Byte), Import Target Community Value, Import Target Extended Community Value, Target AS Value, Target AS Value (4Byte), Target Community Value, Target Extended Community Value,
MPLS Administrative Groups	Displayed Name	Value

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-2 Format and Range policy objects and associated parameters for policies (continued)

Policy	Format policy	Range policy
Static Configuration for SRLGs	Displayed Name	—
Shared Risk Link Group Static Config	Displayed Name	Value
Accounting policy	Description, Displayed Name	ID
File policy	Description, Displayed Name	ID
Maintenance Domain	Description, Name	MD Mgr ID
Network Address Translation policy	Description, Displayed Name	—
PAE 802_1x policy	Description, Displayed Name	—
RADIUS Based Accounting	Description, Displayed Name	—
RMON	Description, Displayed Name	—
Time of Day Suite	Description, Name	—
Time Range	Description, Name	—
VRRP policy	Description, Displayed Name	ID, Service ID

21.10 What are the system preferences configuration procedures?

21.10.1 Description

The following procedures describe how to set parameters that globally define NFM-P operation, such as GUI display options, operational thresholds, and aspects of network management.

21.11 How do I set the NFM-P system preferences?

CAUTION

Service Disruption

A system preference setting typically applies globally to an NFM-P system; changing a system preference setting may adversely affect NFM-P operation.

Contact technical support before you attempt to change a System Preferences setting.

Note: Changing a system preference requires a scope of command role with administrator privileges.

21.11.1 Steps

1

Choose Administration→System preferences from the NFM-P main menu. The System Preferences form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The following table lists and describes, by tab, the functions on the System Preferences form, and where to find additional information, if applicable. The table lists the tabs in sequential order of display.

Note: The descriptions in the table are general, and not an exhaustive list of the available settings. Specific System Preferences requirements and settings are described in NFM-P procedures, as required.

Table 21-3 NFM-P system preferences

Tab and available settings	See
General	
GUI form display — tabs shown or hidden by default, whether to allow customization	*NSP NFM-P Classic Management User Guide*
CSV encoding for file export operations	
NE display threshold for equipment groups in navigation tree — maximum NEs displayed in expanded equipment group Equipment groups can contain up to 2000 NEs. The GUI navigation tree display a maximum of 500 NEs per group. You can set the NE display threshold for Equipment Group parameter to accomplish any of the following: • To display all the NEs in equipment groups that contain no more than 500 NEs, set the parameter to 500. • To display a small number of NEs per equipment group, set the parameter to a low value. The minimum setting is 2. You can use the NE list form to access and manage the NEs in the group, and you can show additional NEs in the tree if required. See “To manage NEs in equipment groups on the navigation tree”in the *NSP NFM-P Classic Management User Guide*. • To allow the display of enough NEs to meet your typical requirements while also allowing additional NEs to show in the tree if necessary, set the parameter to a value in the middle of the range. This is useful if you have more than 500 NEs in a group. For example, if the parameter is set to 300, then 300 of the NEs in the group are displayed in the tree. You can select and display up to 200 additional NEs in that group before the limit of 500 is reached. Select the additional NEs to show in the tree from the NE list form for the group; see “To manage NEs in equipment groups on the navigation tree” in the *NSP NFM-P Classic Management User Guide*. You must close and re-open the NFM-P client for changes to the NE display threshold for Equipment Group parameter to take effect. The change is propagated to all GUI clients during the next client startup.	
Services	

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-3 NFM-P system preferences (continued)

Tab and available settings	See
Default behavior for the following service functions: • Composite services: - Allow or suppress the auto discovery of Spoke, CCAG, SCP, or RVPLS connectors. - Enable or disable the use of VRF Route Target connections. - Specify whether service alarms are aggregated in composite services. • Service bandwidth management: - Allow or suppress multi-segment tunnel selection. - Enable or disable Service Bandwidth Management (CAC). • Specify the maximum of sites that can be moved from one service to another when reducing the overall size of a particular service; the default is 25. • Specify the default priority of a service when creating a service; the default is set to Low. • Allow or suppress VPRN SNMP Community string warnings and alarms. • Allow or suppress the automatic removal of an empty service. • Enable or disable the use of multi-segment tunnel selection functionality. • Specify if a site name and description are to be added when a service is created. • Allow or suppress Route Target Reservation alarms. • Enable or disable if a service or service site can be deleted if the service or service site has any child objects such as SAPs, SDP bindings, policies, or any other objects related to the service CLI hierarchy. When enabled, you must first delete all child objects before the service or service site can be deleted. This preference only applies to services or service site associated with SROS-based devices. • Specify if a Service Name is to be added to the Site Name when sites are added to a service.	*NSP NFM-P Classic Management User Guide*
TCA	
Allows you to configure the default behavior associated with configuring TCA policies such as specifying the maximum TCA limit, the TCA reset synchronization time or reset interval, and the default TCA severity.	*NSP NFM-P Classic Management User Guide*
Statistics	
Allows you to configure the default behavior associated when exporting statistics files, such as specifying the log file retention and rollover times.	*NSP NFM-P Statistics Management Guide*
Allows you to enable or disable the database storage of statistics; when database storage is disabled for a statistics type, the statistics data is retained only temporarily on a main or auxiliary server, and must be retrieved using the registerLogToFile XML API method	*NSP NFM-P Statistics Management Guide*
The Accumulate time over suspect intervals parameter specifies how to manage the Periodic Time of the first valid statistics record after a suspect collection of the record. When the parameter is enabled, the Periodic Time of a record increases by the collection interval length after each consecutive suspect collection. Consequently, the periodic data values in the first valid record are averaged over a greater time span to yield a more realistic value.	*NSP NFM-P Statistics Management Guide*
Allows you to configure the number of JMS client connection checks that are performed when exporting statistics files before a registerLogToFile request is automatically de-registered.	*Network Developer Portal*

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-3 NFM-P system preferences (continued)

Tab and available settings	See
Allows you to specify whether the accounting policy ID is included in the header of each accounting file. The function enables an OSS to use XML API filters based on the policy ID, if required.	*NSP NFM-P Statistics Management Guide* *Network Developer Portal*
Bin Alarm	
Allows you to configure the maximum Bin Alarm limit, reset synchronization time, reset interval, and alarm severity.	*NSP NFM-P Classic Management User Guide*
Test Manager	
Allows you to configure the default retention time for dB test results and target test results and log files performed with the Service Test Manager and which test results are stored.	*NSP NFM-P Classic Management User Guide*
User Activity	
Allows you to configure how much user activity log information the NFM-P stores before purging information, and how long to retain the information.	9.7 “What is user activity logging?” (p. 236)
OLC	
Allows you to configure the default behavior associated with OLC state of an object that is undergoing commissioning or maintenance. You can configure the following: • In the Automatic OLC State Change panel, enable or disable the Enable Automatic OLC State change parameter to indicate whether the OLC state is automatically set to maintenance when the following actions occur: - When the Administrative state is down. - If the status of the parent object is set to administratively down. - If the affecting object administrative state is down. If the Enable Automatic OLC State change parameter is enabled, a Shut Down action sets the object OLC state to Maintenance and a Turn Up action sets the object OLC state to In Service. This state change is also applied to any child objects, unless the child object OLC state is locked in maintenance mode. • In the OLC Scheduling panel, for scheduled objects that are set to maintenance mode, enable the Create Info Alarm Prior to OLC Revert, if an info alarm is to be raised prior to an OLC revert and the lead time of the alarm notification before reverting. • In the OLC Scheduling panel, you can customize the three revert times that appear for the Revert OLC State parameter in the in the OLC panel on service and network object properties forms.	21.57 “How do I schedule an OLC state change?” (p. 667)
Policies	

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-3 NFM-P system preferences (continued)

Tab and available settings	See
Allows you to display or hide the policy names on policy configuration forms for the following: • Access ingress and access egress policies • ACL IP, ACL IPv6, and ACL MAC policy filters • QoS network policies	*NSP NFM-P Classic Management User Guide*
Allow you to set a restriction in the distribution mode for certain types of local policies that will permit local editing only. Additionally, the following applies to this system preference configuration: • Policy types supported by this system preference include Access Ingress, Access Egress, Network QoS, ACL MAC, ACL IPv4, and ACL IPv6. • When creating any of these policies, if you set the Scope parameter to exclusive, the NFM-P will set the distribution mode to local edit. • The NFM-P will not allow policies with the Scope parameter set to exclusive to be assigned or used more than once. • If you attempt to set the Policy Distribution Mode to Sync With Global while the Scope attribute is configured as exclusive, an error message will result.	
Allow you to specify that for policy changes made using CLI, to switch the distribution mode for certain types of local policies to Local Edit Only, as opposed to the default Sync with Global mode.	
Allows you to configure the automatic distribution of a global policy to applicable NEs once the policy is released.	
Allows you to configure the maximum number of scheduled audit results stored for a local policy.	
Allows you to enable or disable if all zones are re-synchronized from the node as local edit only. If you disable the Discover Security Zone in Local Edit Only parameter, all zones re-synchronized from the node are set to Sync With Global. • The Discover Security Zone in Local Edit Only parameter is only supported on the 7705 SAR-8 with CSMv2, 7705 SAR-8v2 with CSMv2, 7705 SAR-18, 7705 SAR-H, 7705 SAR-Hc, and 7705 SAR-Wx variants, Release 6.1 R1 or later.	
Custom NE Properties	
Allows you to configure if custom property labels and values are used to identify an NE, for example, the location and site name that differs from the actual NE site name. These properties cannot be configured on the NE. Additionally, the following applies to this system preference configuration: • If custom property labels are not configured, the default labels are used. • NE custom properties support the extended character set including multi-byte characters. • Custom property labels and values are displayed in the following locations: - NE Properties form - NE List form	—
ESM	

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-3 NFM-P system preferences (continued)

Tab and available settings	See
Allows you to configure the default behavior associated with the on-demand retrieval of residential subscriber-related information from NEs such as: • The tracked subscriber retrieval timeout interval • The subscriber host retrieval timeout interval • The maximum number of residential subscriber instances returned via XML API • If managed route information is to be collected • If QoS override information is to be collected • If SLAAC host addresses are to be collected • If access loop encapsulations are to be collected • If BGP peer information is to be collected	*NSP NFM-P Classic Management User Guide*
Multi Vendor	
Allows you to configure the Enforce SysObjectId Validation on Driver Module parameter. The parameter specifies whether a driver replacement will be blocked if the SysObjectIds do not match.	*NSP NFM-P Classic Management User Guide*
MPR	
Allows or denies user-access to configure Wavence devices using a Local Craft Terminal (LCT). This prevents multi-write access sessions on Wavence devices. You can also enable or disable if the NFM-P receives LAC alarms from the nodes.	*NSP Wavence Device Support Guide*
Network Group Encryption	
Allows you to set the NGE version	*NSP NFM-P Classic Management User Guide*

2

Configure the required parameters. Information about system preferences parameters is available from the Parameter Search Tool in the NSP Network Developer Portal.

3

As required, click on the appropriate tab to configure another system preference.

4

Click OK to save your changes and close the form.

END OF STEPS

21.12 How do I create or configure a format policy?

21.12.1 Steps

1

Choose Administration→Format and Range Policies from the NFM-P main menu. The Format

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

and Range Polices form opens.

2

Expand Format/Range (Property Rules) and choose Format Policy (Property Rules) from the Select Object Type drop-down menu.

3

Click Create or choose a format policy and click Properties. The Format Policy (Create | Edit) form opens.

4

Configure the required parameters.

5

Select an object and property for which you need to apply the name format policy in the Property panel.

6

Click on the Users tab.

Note: Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more format policies to a user or user group.

7

Click Add. The Select User form opens with a list of users.

8

Select one or more users in the list and click OK. The Format Policy form is refreshed with the selected users.

9

Click on the User Groups tab.

10

Click Add. The Select Group form opens with a list of user groups.

11

Choose one or more user groups in the list and click OK. The Format Policy (Create | Edit) form is refreshed with the selected user groups.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12

Click on the Text Block Formats tab to further define the format of the text. For example, an operator can classify a group of services with a similar name. The operator can also create a tool tip text to describe the purpose of the parameter.

13

Click Move Up or Move Down to change the sequence of the text blocks in the text string.

14

Click Create and perform one of the following:

a. Choose Auto-Filled Parameter. The Auto-Filled Parameter (Create) form opens.

b. Choose Masked Text Parameter. The Formatted Text (Create) form opens.

c. Choose Number Range Parameter. The Number Range (Create) form opens.

d. Choose Text Parameter. The Text (Create) form opens.

15

Configure the required parameters.

The Min. Length and Max. Length parameters are not configurable when the Read Only parameter is enabled.

16

Save your changes and close the forms.

Note: After a format policy is applied to a service, a drop-down menu is displayed beside the object field during object creation, to indicate that a format policy is in effect. When there is only one matching policy, the drop-down menu is dimmed. When there are multiple matching policies, the drop-down menu is used to choose a policy. The sequence of the policies in the drop-down menu is based on the value of the Priority parameter.

END OF STEPS

21.13 How do I create or configure a range policy?

21.13.1 Steps

1

Choose Administration→Format and Range Policies from the NFM-P main menu. The Format and Range Polices form opens.

2

Expand Format/Range (Property Rules) and choose Range Policy (Property Rules) from the Select Object Type drop-down menu.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Click Create or choose a range policy and click Properties. The Range Policy (Create | Edit) form opens.

4

Configure the required parameters.

5

Select an object and property for which you need to apply the range policy in the Property panel.

6

Configure the parameters in the Range panel.

7

Configure the parameters in the Auto Assignment panel.

8

Click on the Users tab.

Note: Only users and user groups that are assigned to this policy are affected by the policy. You can apply one or more range policies to a user or user group.

9

Click Add. The Select User form opens with a list of users.

10

Choose one or more users in the list and click OK. The Range Policy form is refreshed with the users.

11

Click on the User Groups tab.

12

Click Add. The Select Group form opens with a list of user groups.

13

Choose one or more user groups in the list and click OK. The Range Policy form is refreshed with the user groups.

14

Click OK and close the forms.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: After a range policy is applied to a service, a drop-down menu is displayed beside the object field during object creation, to indicate that a range policy is in effect. When there is only one matching policy, the drop-down menu is dimmed. When there are multiple matching policies, the drop-down menu is used to choose a policy. The sequence of the policies in the drop-down menu is based on the value of the Priority parameter.

END OF STEPS

21.14 How do I modify the base configuration of all GUI clients?

Note: You can exclude a specific NFM-P client from a global configuration change by using a command line option when you open the client GUI.

21.14.1 Steps

1

Log in to the NFM-P main server station as the nsp user.

2

Modify the appropriate client configuration file in the /opt/nsp/nfmp/server/nms/config/clientDeploy directory. For example, update the nms-client.xml file with a new client log location.

3

Open a console window.

4

Enter the following to enable an update notification for clients that connect to the server and to prepare the client configuration files for download.

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsdeploytool.bash deploy ↵
```

5

Close the console window.

6

Perform one of the following on each single-user GUI client and client delegate server station.

Note: When you perform this step on a client delegate server station, you affect each GUI client that connects through the client delegate server.

a. Update the client configuration by restarting the client GUI. The client automatically backs up the current configuration and applies the configuration change.

Note: On a RHEL client delegate server station, you must start the client software as the root user, or the configuration update fails.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

On RHEL, the client configuration backup is stored in the *path*/nms/configBackup directory, where *path* is the client installation location, typically /opt/nsp/client.

On Windows, the client configuration backup is stored in the *path*\nms\configBackup directory, where *path* is the client installation location, typically C:\nsp\client.

b. Retain the current client configuration when the client GUI starts by specifying the startup option that disables the auto-client update function. See “Procedures for opening and closing the GUI” in the *NSP NFM-P Classic Management User Guide* for information about GUI client startup options.

Note: Specifying a client startup option affects only the current GUI session. To ensure that the client configuration is not updated automatically during a subsequent session, you must open the session using the startup option that disables the auto-client update.

END OF STEPS

21.15 How do I change the default user file locations on a client delegate server?

21.15.1 Purpose

Perform the procedure to configure the default location of one or more of the following on an NFM-P client delegate server:

- user preference files that contain the following information:
  - saved table layouts
  - preferences saved using Application→User Preferences
- script result files

21.15.2 Steps

1

Close each GUI client that connects through the client delegate server by choosing Application→Exit from the NFM-P main menu.

2

Log in to the client delegate server station as the nsp user.

3

Open a console window.

4

Navigate to the client configuration directory, typically /opt/nsp/client/nms/config on RHEL, and C:\nsp\client\nms\config on Windows.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Open the nms-client.xml file using a plain-text editor.

6

To change the default GUI preferences and table layout file location, insert the following line directly above the </configuration> line at the end of the file:

```
guiPreferences path="new_file_location" />
```

where *new_file_location* is the new default GUI table layout and GUI preferences location

Note: The specified location can be an absolute file path, or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location.

7

To change the default script result file location, insert the following line directly above the </configuration> line at the end of the file:

```
cache directoryName="new_file_location" />
```

where *new_file_location* is the new default script result file location

Note: The specified location can be an absolute file path, or a file path relative to *install_dir*/nms, where *install_dir* is the client installation location.

8

Save and close the nms-client.xml file. Subsequent client GUI sessions on the client delegate server use the new file location.

END OF STEPS

21.16 How do I enable main database backup file synchronization?

21.16.1 Purpose

Perform the procedure to enable the main servers in a redundant NFM-P system to synchronize the main database backup file sets. After a database backup, if database backup file synchronization is enabled, the NFM-P automatically copies the database backup file set to the standby database station.

Note: The procedure applies only to a redundant NFM-P system.

Note: Before you perform the procedure, you must ensure that there is sufficient network bandwidth between the main database stations for a database copy operation. See the *NSP NFM-P Planning Guide* for information about the bandwidth requirements of database backup file synchronization.

Note: You must perform the procedure first on the standby main server station, and then on the primary main server station.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.16.2 Steps

1

Log in to the main server station as the root user.

2

Open a console window.

3

Enter the following:

```
# samconfig -m main ↵
```

The following is displayed:

```
Start processing command line inputs...
<main>
```

4

Enter the following:

```
<main> configure redundancy database backup-sync ↵
```

The prompt changes to `<main configure redundancy database>`.

5

Enter the following:

```
<main configure redundancy database> exit ↵
```

The prompt changes to `<main>`.

6

Enter the following:

```
<main> apply ↵
```

The configuration change is applied.

7

Enter the following:

```
<main> exit ↵
```

The samconfig utility closes.

8

Enter the following to switch to the nsp user:

```
# su - nsp ↵
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

9

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

10

Enter the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server puts the configuration change into effect. The NFM-P automatically copies subsequent main database backup file sets from the primary database station to the standby database station.

11

Close the console window.

END OF STEPS

21.17 How do I modify the default time period of statistics displayed by the Statistics Manager search filters?

21.17.1 Purpose

By default, the NFM-P Statistics Manager limits search results to statistics records collected during the past hour. Perform the procedure to modify the default time period of the statistics displayed by the NFM-P Statistics Manager search filters.



CAUTION

Service Disruption

Consider possible service disruptions before modifying the statistics default time period.

Changing the default time period for the NFM-P Statistics Manager search filters can affect the performance of the NFM-P.

21.17.2 Steps

1

Choose Application→Exit to close the NFM-P client GUI, if it is open.

2

Navigate to the client configuration directory, typically /opt/nsp/client/nms/config on RHEL, and C:\nsp\client\nms\config on Windows.

3

Open the nms-client.xml file using a text editor.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Locate the section that begins with the following XML tag:

```
<statistics
```

5

Edit the following line to read:

```
browserDefaultHour="value"
```

where *value* is the default number of hours for the Past <number_of_hours> filter

6

Save the changes and close the file.

7

Log in to an NFM-P GUI client to verify that the new value is displayed on the Statistics Manager form.

END OF STEPS

21.18 How do I modify the default time period of statistics displayed on object properties forms?

21.18.1 Purpose

By default, the NFM-P displays the statistics records collected during the past hour on the Statistics tab on object properties forms. Perform the procedure to modify the default time period of the statistics displayed on the Statistics tab of an object properties form.



CAUTION

Service Disruption

Consider possible service disruptions before modifying the statistics default time period.

Changing the default time period for the NFM-P Statistics Manager search filters can affect the performance of the NFM-P.

21.18.2 Steps

1

Choose Application→Exit to close the NFM-P client GUI, if it is open. The NFM-P client GUI closes.

2

Navigate to the client configuration directory, typically /opt/nsp/client/nms/config on RHEL, and C:\nsp\client\nms\config on Windows.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Open the nms-client.xml file using a text editor.

4

Locate the section that begins with the following XML tag:

```
<statistics
```

5

Edit the following line to read:

```
tabDefaultHour="value"
```

where *value* is the default number of hours for the Past <number_of_hours> filter

6

Save the changes and close the nms-client.xml file.

7

Log in to an NFM-P GUI client to verify that the new value is displayed on the Statistics tab of an object properties form.

END OF STEPS

21.19 How do I enable the preservation of the XML API statistics pool size?

21.19.1 Purpose

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Perform this procedure to ensure that the pool size for XML API statistics operations is not reset by a system upgrade or main server configuration update.

Note: You must perform the procedure on each main server in the NFM-P system.

21.19.2 Steps

1

Log in to the main server station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Locate the following line:

```
<deploymentWorker statsPoolSize="nn"
```

7

Add the following to the end of the line:

```
preserveAttributes="true"
```

The line now reads:

```
<deploymentWorker statsPoolSize="nn" preserveAttributes="true"
```

8

Save and close the file.

9

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

10

Enter of the following:

```
bash$ ./nmsserver.bash read_config ↵
```

The main server configuration is updated.

11

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.20 How do I configure auto-assigned service ID ranges and uniqueness checking?

21.20.1 Purpose



CAUTION

Service Disruption

Modifying the NFM-P system configuration can have serious consequences that include service disruption.

Contact technical support before you attempt to modify the server configuration.



CAUTION

Misconfiguration risk

You must configure each main server in the NFM-P system using the same values, as described in the procedure; otherwise, a potentially service-affecting configuration mismatch exists.

If you perform the procedure, ensure that you perform the procedure on each main server station.

By default, the NFM-P performs uniqueness checking to verify that a service ID that is to be auto-assigned is not currently associated with a service in the NFM-P managed network. Service creation using auto-assigned service IDs can take considerable time, and consume system resources unnecessarily, if the NFM-P manages a large number of services.

To avoid such a scenario, you can configure a range of service IDs for auto-assignment, and disable the uniqueness checking for the specified range.

Perform this procedure to :

- configure the system-wide default minimum and maximum values for auto-assigned service IDs
- disable or enable the uniqueness checking of service IDs during service creation

Note: When uniqueness checking is disabled for a range, a value in the range cannot be used as a service ID for the following. or an error is logged and the service creation fails:

- manually created service
- service created using a range policy, if the ranges in the range policy and server configuration overlap to any extent

Note: The order in which you configure the main servers is unimportant, but you must perform the procedure on each main server before you attempt automatic service creation using the specified service ID range.

21.20.2 Steps

1

Log in to the main server station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Locate the section that begins with the following line:

```
<idManager>
```

The section describes the ID ranges for which you can configure the minimum and maximum values.

7

Add a serviceId range entry with uniqueness checking disabled to the <idManager> section, for example:

```
<range
        name="serviceId"
        min="minimum_value"
        max="maximum_value"
        skipIdCheck="true" />
```

Note: The skipIdCheck parameter can have one of the following values:

- true—disables the uniqueness check
- false—enables the uniqueness check

Note: Before you set skipIdCheck to true for a service ID range, you must ensure that no existing service in the NFM-P managed network has a service ID in the range.

8

Save and close the file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The NFM-P puts the configuration change into effect.

10

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P alarm administration

21.21 What are alarm thresholds?

21.21.1 Escalation and de-escalation thresholds

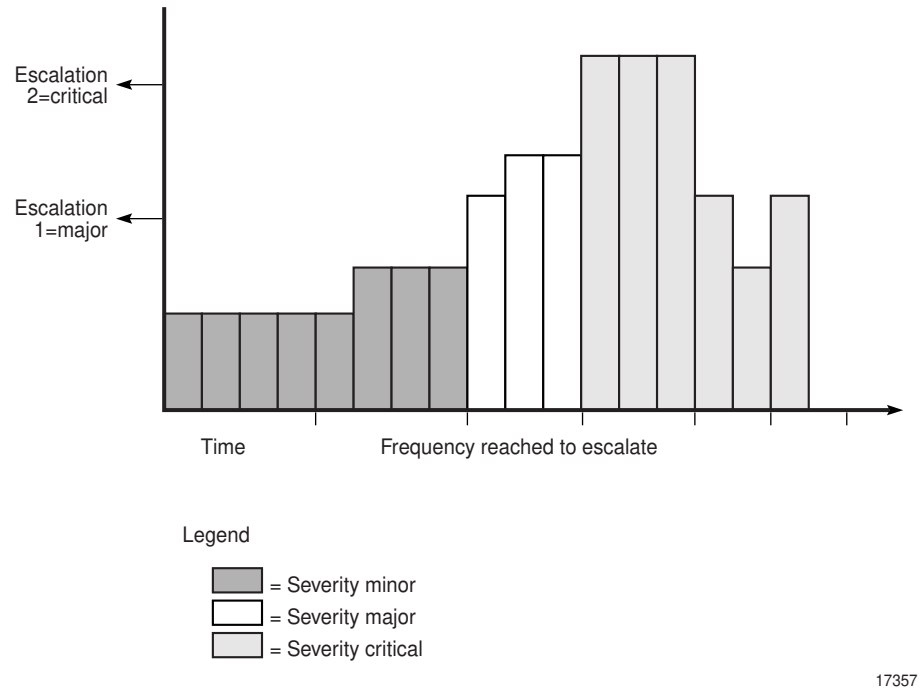
For alarms that occur repeatedly, you can set thresholds in an alarm policy to escalate and de-escalate the severity of the alarm; see 21.27 “How do I configure alarm policies?” (p. 629). Escalation to a higher severity can alert you to a problem when an alarm is occurring too often, or occurs too many times. De-escalation restores a lower level of severity when the alarm occurs less often. Configured thresholds are applied immediately once the updated policy is saved.

You can set more than one escalation threshold and de-escalation threshold in a policy, so severity for a particular alarm type can be increased or decreased more than once if required.

You can configure any higher severity level for escalation, and any lower level for de-escalation; it doesn’t have to be an adjacent severity level.

Figure 21-1, “Alarm escalation without de-escalation” (p. 623) shows how an escalation policy will increase the severity setting of an alarm based on a specified frequency threshold. The severity is increased twice: from minor to major, and then from major to critical, based on two threshold values for the Frequency parameter. In this case, no de-escalation threshold is applied, so the alarm remains at critical severity even when the frequency falls below the threshold again.

Figure 21-1 Alarm escalation without de-escalation

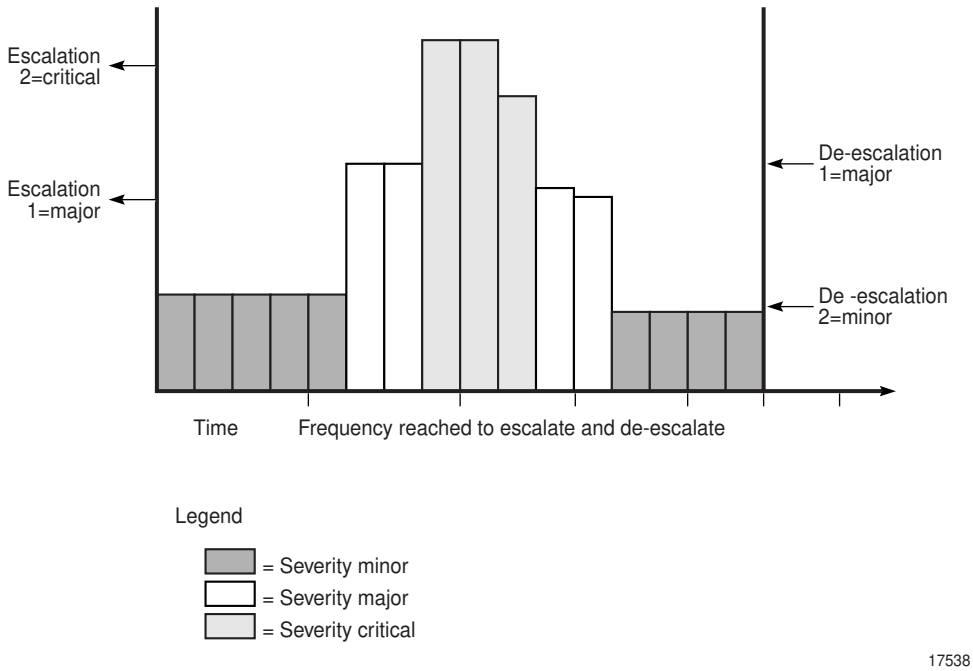


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: When no de-escalation policy is applied, escalated alarms are not de-escalated once the frequency of the alarm is less than the alarm escalation threshold.

Figure 21-2, “Alarm escalation and de-escalation” (p. 623) shows changes in alarm severity when both escalation and de-escalation frequency thresholds are applied. An alarm reaches two configured frequency thresholds and is escalated twice: from minor to major, and from major to critical. Then, when the frequency reaches the specified values for de-escalation, the alarm severity is reduced again.

Figure 21-2 Alarm escalation and de-escalation



Escalation thresholds can be based on frequency of occurrence of an alarm, or total number of occurrences, or both.

- The **Frequency** threshold is the number of times an alarm occurs within a specified interval. The default interval for an alarm policy is 24 hours, but you can modify this using the Interval parameter on the Specific Alarm Policy form. The NFM-P uses an internal mechanism to assess the frequency threshold each time the alarm occurs, so it is not necessary to wait for the full interval to elapse before escalation/de-escalation is triggered.
- The Occurrence threshold is the total number of occurrences of the alarm since the policy was applied; that is, since the default value of zero for the Occurrence parameter was changed for the policy. When the total number of occurrences of an alarm reaches this threshold, the alarm is escalated to the configured severity.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If the Occurrence threshold is deleted from a policy, existing alarms remain at their escalated severity. However, the next occurrence and all subsequent occurrences will show the severity configured in the Initial Severity Assignment (unless they reach another configured threshold).

Frequency and Occurrence thresholds are independent of each other; the alarm is escalated when either of the thresholds is reached. At least one of the thresholds (Frequency or Occurrence) must be set to a value other than zero for escalation to occur. If a value is set to zero then that threshold is ignored and no escalation occurs for that threshold.

De-escalation thresholds are based only on frequency. If the Frequency parameter is set to zero then the threshold is ignored for frequency changes and no de-escalation occurs.

You must enable the Escalation and De-Escalation check boxes on the Specific Alarm Policy form for their associated thresholds to be applied.

Additionally, policy-based escalation and de-escalation is controlled on the Alarm Settings form, General tab. You must enable the Allow Policy Based Escalation and Allow Policy Based De-escalation parameters in the Alarm Severity Settings panel, in the Automatic sub-panel; see 21.28 “How do I configure alarm severity and deletion behavior?” (p. 631).

Acknowledging an alarm does not affect escalation policies. Deleting an alarm affects the frequency counter; see 21.28 “How do I configure alarm severity and deletion behavior?” (p. 631).

Escalation policies are affected by the Auto Deletion Rule parameter of the global alarm deletion policy. See 21.28 “How do I configure alarm severity and deletion behavior?” (p. 631) for more information. When an escalation policy uses the “Delete Alarms when Cleared” default option for the Automatic Alarm Deletion Settings parameter, the escalation policy is not applied, unless alarm debouncing is enabled for the particular alarm type. You must configure the parameter to a value other than “Delete Alarms when Cleared” to ensure that the escalation policy is applied.

21.22 What is alarm suppression?

21.22.1 Overview

The NFM-P is designed to not generate alarms when numerous SNMP traps are sent in quick succession for the same type of event. This prevents alarm storms during intermittent outages in the network caused by bouncing NEs; for example, if links go up and down rapidly. The NFM-P continues to resynchronize the network. If the bouncing NEs continue to send down state SNMP traps, the NFM-P eventually receives the trap and generates the appropriate alarm.

To indicate how often an alarm is generated, the number of occurrences of each instance of the alarm is tracked in the alarm record of the initial alarm. Click on the Statistics tab of an Alarm Info form to display how often the alarm was generated.

To escalate the alarm severity if an alarm reoccurs a specific number of times, use the threshold crossing alert functionality. Configure the escalation or the de-escalation parameter as described in 21.27 “How do I configure alarm policies?” (p. 629) .

The NFM-P uses a trap throttling process to prevent the NFM-P system from being overloaded with traps if a failure occurs. Trap throttling does not affect the sequencing of traps. The trap throttling process allows the NFM-P to process traps when time permits. As a result, the NFM-P keeps track of the traps that the software missed and resynchronizes only the missed traps. Trap throttling is

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

supported and configured using the CLI on each Nokia NE. See the NE System Management Guides for configuration information.

21.23 What is the alarm purge algorithm?

21.23.1 Overview

Because a large number of outstanding alarms can affect system performance, the NFM-P purges outstanding alarms. The alarm purge algorithm sorts alarms using the following criteria:

- lower severity alarms are deleted before higher severity alarms
- within a severity, the oldest alarms are always deleted first

Note: The alarm purge algorithm is not applied to the following correlating—or root cause—alarms unless the red threshold has been crossed:

- EquipmentRemoved
- EquipmentMismatch
- EquipmentDown
- EquipmentAdministrativelyDown
- ContainingEquipmentMissing
- ContainingEquipmentMismatch
- ContainingEquipmentAdministrativelyDown
- ContainingEquipmentOperationallyDown
- TunnelDown
- TunnelAdministrativelyDown
- AccessInterfaceDown
- SdpBindingDown

When an alarm policy does not exist, the NFM-P purges alarms as follows:

For collocated systems:

- If the outstanding alarm count reaches 45 000, the NFM-P:
  - raises an alarm to indicate that an alarm purge is in progress
  - purges non-critical alarms not in the exclusions list to the historical alarm log until the count drops to 45 000
- If the outstanding alarm count reaches 60 000, the NFM-P:
  - raises an alarm to indicate that an alarm purge is in progress
  - purges alarms to the historical alarm log, starting with the oldest lowest severity alarms, until the count drops to 45 000
  - displays “Max alarm count exceeded” in the status bar

For distributed systems:

- If the outstanding alarm count reaches 200 000, the NFM-P:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

  - raises an alarm to indicate that an alarm purge is in progress
  - purges non-critical alarms not in the exclusions list to the historical alarm log until the count drops to 200 000
- If the outstanding alarm count reaches 250 000, the NFM-P:
  - raises an alarm to indicate that an alarm purge is in progress
  - purges alarms to the historical alarm log, starting with the oldest lowest severity alarms until the count drops to 200 000
  - displays “Max alarm count exceeded” in the status bar

To ensure that purged alarms are logged, you must enable alarm history logging. See 21.29 “How do I configure alarm history logging?” (p. 632) for information about configuring alarm history logging and purging policies.

21.24 What is automatic deletion of correlated alarms?

21.24.1 Overview

You can configure the NFM-P to automatically delete correlated alarms when the correlating alarm is deleted, as described in 21.28 “How do I configure alarm severity and deletion behavior?” (p. 631). You can also configure NFM-P alarm settings to specify whether a user notification is displayed before you delete one or more correlated alarms.

To prevent cleared alarms from persisting in the NFM-P, alarm severity is not promoted by alarm correlation when you choose one of the following options for automatic alarm deletion. The options disable the correlation of alarm severity in the NFM-P network.

- Disable Automatic Alarm Deletion
- Delete Alarms when Acknowledged
- Delete Alarms when Cleared and Acknowledged

Note: A correlated alarm is not deleted after the deletion of the correlating alarm if there is another correlating alarm associated with the correlated alarm. Therefore, the number of correlated alarms that are automatically deleted may be less than the number in the warning notification to a GUI operator.

21.25 What is alarm debouncing?

21.25.1 Overview

Bouncing alarms, or flapping alarms, occur when an alarm is raised and cleared several times by the network within a short period of time. For example, an alarm can be generated several thousand times in a 24–hour period. When an alarm is generated, the alarm is typically cleared very shortly after being raised.

Alarm debouncing using the NFM-P allows you to detect and reduce the number of deleted, or cleared, alarms that are logged in the historical database, while allowing alarm events and related statistics to be kept up to date.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

You can configure debouncing on alarm policies for implicitly cleared alarms only, that is, alarms which are automatically cleared by the NFM-P when a condition is met. You can configure alarm debouncing only on policies for which the auto-deletion rule cannot be configured, in which case "N/A" appears under the Auto Deletion Rule column on the Policies tab of the Alarms Settings form. Alarm debouncing is not configurable for policies for which No Deletion Rule or a configured deletion rule appears under the Auto Deletion Rule column on the Policies tab of the Alarm Settings form.

Although alarm events that occur are processed normally when alarm debouncing is enabled, alarm clear events that occur are not processed immediately. The alarm clear events are held in a separate cache until the hold period, which you configure in the debouncing policy, has elapsed. If another clear event occurs before the hold period has elapsed for the previous clear event of the same alarm, the more recent clear event replaces the older clear event in the cache. After the hold period has elapsed, the alarm clear event is removed from the cache, queued and processed.

If an alarm clear event is on hold in the cache and an alarm raise event for that same alarm is received, the clear event is removed from the cache and dropped. Because the alarm was not cleared and not raised again, the raise event is processed as an update event and the existing alarm instance is updated.

When an escalation policy uses the "Delete Alarms when Cleared" default option for the Automatic Alarm Deletion Settings parameter, the escalation policy is not applied, unless alarm debouncing is enabled for the particular alarm type. See 21.28 "How do I configure alarm severity and deletion behavior?" (p. 631) for more information about how to configure escalation policies.

See 21.31 "How do I configure alarm debouncing ?" (p. 634) for information about how to configure alarm debouncing policies.

21.25.2 Purging the debouncing cache

By default, up to 5000 clear events for different alarms can be held in the debouncing cache at one time.

When the alarm debouncing cache reaches capacity with excess bouncing alarms, the NFM-P raises the AlarmDebouncingThresholdReached alarm. When this occurs, alarm debouncing is temporarily disabled and at least 70% of the alarm clear events that are being debounced are processed immediately. Alarm debouncing is re-enabled after the processing of cached events completes.

21.25.3 XML API and alarm debouncing

When debouncing is enabled, JMS listeners handle alarm events received differently from when debouncing is disabled. For example, when a raise/clear raise/clear raise/clear sequence occurs when debouncing is not enabled, JMS listeners receive and handle one update event, but the three clear events are processed by the NFM-P, and three historical alarms are logged. When this sequence occurs when debouncing is enabled, JMS listeners receive and handle a raise, update, update, clear, and only one clear event is processed by the NFM-P.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.26 How do I filter alarms for XML API clients using the NFM-P GUI?

21.26.1 Overview

You can use a GUI client to configure an alarm filter for XML API clients. See 21.32 “How do I configure alarm filters for XML API clients?” (p. 634) and the NSP Network Developer Portal.

Consider the following:

- Only public filters can be applied to XML API clients.
- When a user logs in to the NFM-P GUI, filters that were created for XML API applications are not applied to GUI alarms.
- Filters that are applied using the NFM-P GUI apply only to the fault (5620-SAM-topic-xml-fault) and filter (5620-SAM-topic-xml-filtered) JMS topics.
- When the NFM-P GUI is used to apply or remove a filter, you do not need to disconnect or reconnect an XML API session.
- When a filter is defined and enabled, and the client does not have an XML API connection, the filter is applied when the XML API client connects.
- When a filter is defined and enabled, and the user has one or more XML API connections, the filter is applied to all of the user XML API connections.
- When an alarm filter is in use with an XML API session and an NFM-P operator changes the contents of the filter, the NFM-P user is informed that the filter is in use and who is using the filter. The NFM-P user is prompted with the option to save the change or cancel the change.
- Alarm filters that are applied to XML API sessions appear in the Sessions tab on the NFM-P User Security-Security Management form.

21.27 How do I configure alarm policies?

21.27.1 Purpose

The NFM-P provides default alarm policies for alarms. You can modify the default settings of these policies.

Perform the following procedure to modify the initial severity assignment, assign urgency levels, enable alarm history, add custom text, and configure other settings for one or more alarm types.

For specific alarm types, you can set thresholds for escalation and de-escalation of alarm severity; see 21.21 “What are alarm thresholds?” (p. 623).

21.27.2 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form opens.

2

Click on the Policies tab and perform one of the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

a. Configure settings for a specific alarm policy, including escalation and de-escalation thresholds, if required. Go to Step 3 .

b. Configure settings for multiple alarm policies. Go to Step 9 .

Note: You cannot configure alarm thresholds for multiple policies at the same time.

3

Choose an alarm type. The alarm types are listed by *policyGroup.AlarmPolicy*.

Note: You can determine the applicable alarm policy for an alarm by searching for the base alarm name in the *NFM-P Alarm Search Tool*. The name format is *package.AlarmName*. For example, the GlobalAppProfileCreated alarm search result shows that the alarm is associated with the aapolicy.GlobalAppProfileCreated policy.

4

Click Properties. The Specific Alarm Policy (Edit) form opens.

5

Configure the required parameters on the General tab.

6

Configure escalation thresholds for the alarm type.

1. Enable the Escalation parameter.
2. Choose a threshold in the list and click Properties, or click Add. The Escalation Threshold form opens.
3. Configure the required parameters.

   For the Frequency parameter, the interval used is displayed on the form. The Interval parameter is configured in Step 5.

   You can configure both Frequency and Occurrence in the same escalation threshold.

   The Severity parameter specifies the severity level the alarm will be escalated to, and must be a higher severity than the Initial Severity Assignment configured in Step 5.
4. Click OK to close the Escalation Threshold form.
5. Configure additional thresholds as required.

7

Configure de-escalation thresholds for the alarm type.

1. Enable the De-escalation parameter.
2. Choose a threshold in the list and click Properties, or click Add. The De-Escalation Threshold form opens.
3. Configure the required parameters.

   For the Frequency parameter, the interval used is displayed on the form. The Interval parameter is configured in Step 5.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The Severity parameter specifies the severity level the alarm will be de-escalated to.

4. Click OK to close the De-Escalation Threshold form.
5. Configure additional thresholds as required.

8

Go to Step 12 .

9

Shift-click to choose multiple alarms. The alarm types are listed by *policy group*.*alarm policy*.

Note: When you attempt to modify the configuration of multiple alarm policies at one time, the configuration is limited to the elements that the alarm policies have in common.

10

Click Properties. The Specific Alarm Policy (Edit) form opens.

11

Configure the required parameters on the General tab.

12

Save your changes and close the forms.

END OF STEPS

21.28 How do I configure alarm severity and deletion behavior?

Note: You must have a user account with the administrator scope of command role or write access to the fm.GlobalPolicy class to perform this procedure.

21.28.1 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form opens.

2

In the Alarm Severity Settings panel, enable or disable alarm severity settings and specify the behavior for automatic and manual alarm settings.

Use the following steps:

1. Configure the Enable Severity Settings parameter, as required. You cannot configure additional parameters in the Alarm Severity Settings panel unless the parameter is enabled.
2. Configure the required parameters in the Manual panel.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3. Configure the required parameters in the Automatic panel.

3

CAUTION

Service Disruption

Deleting an alarm resets the frequency of the alarm to 1.

This may cause conflicts with configured alarm escalation and de-escalation policies.

In the Alarm Deletion Settings panel, enable or disable alarm deletion settings and specify the behavior for manual and automatic alarm deletion settings.

1. Configure the Enable Deletion Settings parameter. You cannot configure parameters in the Alarm Deletion Settings panel unless the parameter is enabled.
2. Configure the other parameters in the Alarm Deletion Settings panel, as required.

4

See 21.29 “How do I configure alarm history logging?” (p. 632) for information about configuring parameters in the Alarm History DB Behavior panel.

5

Configure the Alarm Event Settings.

6

To reset all parameters on the General tab to their default values, click Reset To Default.

7

Save your changes and close the form.

END OF STEPS

21.29 How do I configure alarm history logging?

21.29.1 Purpose

The NFM-P stores alarms in the alarm history database for record-keeping and trend analysis. You can specify when alarms are logged to the alarm history database.

Note: When the maximum number of alarms allowed in the alarm history database is reached, the NFM-P deletes the oldest alarms. If you need to save information about the alarms, save a file that contains the alarm log information, as described in the *NSP NFM-P Classic Management User Guide*.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.29.2 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form opens.

2

Configure the required parameters in the Alarm History DB Behavior panel.

Note: Nokia recommends that you enable the Log On Deletion parameter to ensure that the alarm history log records all deleted alarms.

3

To reset all parameters on the General tab to their default values, click Reset To Default.

4

Save your changes and close the form.

END OF STEPS

21.30 How do I show or hide the alarm Additional Text button?

21.30.1 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form opens.

2

Click on the Additional Text tab and enable or disable the Show Additional Text Button on Properties Forms parameter.

3

Save your changes and close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.31 How do I configure alarm debouncing ?

21.31.1 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form opens.

2

Click on the Policies tab and choose one or more alarm policies. In the policies table, only policies which show “N/A” under Auto Deletion Rule are configurable with alarm debouncing. If you select one or more alarm policies for which the Auto Deletion Rule parameter is a value other than “N/A”, the alarm debouncing parameters do not appear.

3

Choose the policy and click Properties. The Specific Alarm Policy (Edit) form opens.

Note: You can also open the Specific Alarm Policy (Edit) form from the Alarm Info form, by clicking on the View Policy button.

4

Configure the Enable Alarm Debouncing parameter.

5

Configure the Hold Period (seconds) parameter to specify the debouncing time interval. If you are enabling alarm debouncing for this policy for the first time, the default value is automatically set to 180. If alarm debouncing was previously enabled, then disabled, the value of the Hold Period (seconds) parameter remains as the last configured value.

6

Save and close the forms.

END OF STEPS

21.32 How do I configure alarm filters for XML API clients?

21.32.1 Purpose

Perform this procedure to configure a filter to control or limit the alarms that the NFM-P forwards to XML API clients over JMS. See 21.26 “How do I filter alarms for XML API clients using the NFM-P GUI?” (p. 629) and the NSP Network Developer Portal for more information.

Note: In order to perform the procedure, you require a user account with XML API access.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.32.2 Steps

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NSP NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Users tab.

3

Choose a user from the list and click Properties. The User (Edit) form opens.

4

In the XML API Session panel, click Select to assign a public alarm filter. The Select Public Alarm Filter for XML API form opens.

5

Perform one of the following:

a. Select a filter in the list. Go to Step 6 .

b. Create an alarm filter.

Use the following steps:

1. Click Create. The Create AlarmObject Filter form opens.
2. Configure an appropriate filter for the XML API client by selecting a filter from the Attribute parameter pull-down menu. You can modify the filter string to meet the operational requirements for an XML API client by configuring the Function, Value, and Operators pull-down menus as appropriate.
3. Click Add to add the filter.
4. Add additional filter criteria for the alarm filter as required.
5. Click Save. The Save Filter form opens.
6. Configure the required parameters.

   Note:

   The Public parameter must be enabled. Only public filters are applied to XML API clients.
7. Save your changes and close the Save Filter and Select Public Alarm Filter for XML API forms.

6

Choose the newly created filter from the list, and click OK. The Select Public Alarm Filter for XML API-User form closes, and the selected filter is applied.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Save your changes and close the forms.

END OF STEPS

21.33 How do I reload all alarms from the historical alarm database?

21.33.1 Purpose

The NFM-P uses an alarm service to cache alarm information. To ensure the cache is current with all alarms stored in the historical alarm database, administrators can reload all alarms from the database. To perform this procedure, you must have a user account with the administrator scope of command role or a scope of command role with write access permissions to the fm.FaultManager class.

CAUTION

Service Disruption

After the procedure is complete, client GUI users viewing open alarm forms and windows may have out-of-date information. Operators must close all open windows and forms, then relaunch -open the windows or forms. This includes windows and forms that display alarm status information, for example, the navigation tree.

21.33.2 Steps

1

Choose Administration→Reload Alarm Information from the NFM-P main menu.

2

Click OK to confirm you are aware that all other users will be affected by the alarm reload.

Alarm information is reloaded and all active client GUIs are updated with the confirmation message that the alarms have been reloaded. Client GUI users can close and then reopen the Alarm Window to refresh the information.

END OF STEPS

21.34 How do I manually escalate or de-escalate the severity of an alarm on the NFM-P?

21.34.1 Purpose

Operators with the appropriate scope of command permissions can promote or demote the severity of alarms when alarm settings are configured appropriately. See 21.28 “How do I configure alarm severity and deletion behavior?” (p. 631) for more information about configuring global alarm settings.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.34.2 Steps

1

Perform one of the following to open the Severity Assignment form:

a. From the dynamic alarm list:

Use the following steps:

1. Filter the alarms. See the *NSP NFM-P Classic Management User Guide* for information about creating search filters.
2. Right-click on an alarm in the list and choose Assign Severity. The Severity Assignment form opens and displays the selected alarm(s).

b. From the alarm list on the Faults tab of the object properties form:

Use the following steps:

1. Open the object properties form for the required object.
2. Click on the Faults tab.
3. Click on a sub-tab. A list of object alarms appears.
4. Filter the alarms. See the *NSP NFM-P Classic Management User Guide* for information about creating alarm filters.
5. Right-click on an alarm in the list and choose Assign Severity. The Severity Assignment form opens and displays the selected alarm(s).

Note: You can choose multiple alarms at the same time. When you choose multiple alarms, the new severity level is applied to all selected alarms.

2

Configure the Assigned Severity parameter.

Note: Before you close the form, you can click Reset to restore the original severity setting.

3

Save the changes and close the forms.

END OF STEPS

21.35 How do I optimize alarm event notifications?

21.35.1 Purpose

The alarm event buffer receives all alarm events that must be broadcast to JMS clients. For optimization purposes, the buffer fills up alarm events and flushes the queue every 3 seconds. During these 3 seconds, if a creation event is queued followed by a deletion event for that same object, both of these events cancel each other out, and no event is sent. However, the alarm corresponding to the deletion event is still logged into historical alarms.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

You can disable the canceling of creation and deletion event pairs. All of the events are reported to all subscribed JMS listeners and are displayed in the Active Alarm list of each GUI client. When this option is deselected, the user receives a warning that this will impact alarm event processing. If optimization is not enabled, third-party JMS listeners may not be able to manage the increased event rate.

21.35.2 Steps

1

Choose Administration→Alarm Settings from the NFM-P main menu. The Alarm Settings form opens.

2

Ensure the Optimize Alarm Event Notifications parameter is enabled.

3

Save the changes and close the form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P license management

21.36 What are NFM-P licenses?

21.36.1 NFM-P licenses

To enable the options or equipment capacity specified in a new license, you must import the license file on each NFM-P main server, as described in 21.39 “How do I update the NFM-P license in a standalone deployment?” (p. 641) and 21.40 “How do I update the NFM-P license in a redundant deployment?” (p. 642) . If required, you can uncompress a license file and view the license information, which is in XML format.

You can view the current NFM-P license specifications from the NFM-P license information form; see 21.37 “How do I view the NFM-P license information?” (p. 640) for information. The form displays the following, which you can export to a file, if required:

- NFM-P software release and patch level
- main servers associated with the license
- licensed NFM-P feature packages
- number of licensed operator positions, other allowances
- license points consumed and remaining
- extended NE software support

See 21.38 “How do I export the NFM-P license information or create a license point inventory?” (p. 641) for export information.

21.36.2 Managing NE license consumption

When an NFM-P license-point limit is reached, the NFM-P does not discover additional equipment of the type to which the limit applies.

From the NFM-P license information form, you can generate a license inventory file that lists the NFM-P license points consumed per object per managed NE. The objects are ordered by NE site ID and by subscriber type; the information for each includes the following:

- object FDN, for equipment
- associated site ID, for equipment
- licensed product name
- number of license points that the object consumes

See 21.38 “How do I export the NFM-P license information or create a license point inventory?” (p. 641) for information.

License consumption by a specific NE

The license consumption information for a specific NE is viewable from the Inventory tab of the NE properties form. The tab lists the license information for cards, blades, chassis, and other NE equipment. See “Inventory management” in the *NSP NFM-P Classic Management User Guide* for more information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

License consumption by specific equipment

The Manage Equipment form displays license consumption information specific to a type of equipment, for example, a physical card.

21.37 How do I view the NFM-P license information?

21.37.1 Steps

1

To view the NFM-P license information in the client GUI:

Note: You can also list equipment license information for one NE or the entire network using the NFM-P Equipment Manager; see “Inventory management” in the *NSP NFM-P Classic Management User Guide*.

1. Choose Help→License Information from the NFM-P main menu. The NSP Network Functions Manager - Packet License (Edit) form opens.
2. View the license information in the following panels:
   - License Information—basic license and system information
   - Feature Packages—installed NSP feature packages
   - Options—optional management function capacities
   - Licensed Limits—the number of consumed and remaining license points for capacity-based licensing objects such as equipment
3. A highlighted entry in the Licensed Limits panel is alarmed, and may indicate that the license capacity is approaching or has reached the license limit. To view the current alarms against an entry, double-click on the entry and click on the Faults tab of the form that opens.
4. Close the open forms, as required.

2

CAUTION

Service Disruption

An NFM-P license file is digitally signed. If you rename or modify the license XML file, the NFM-P rejects the license.

Do not rename or modify the XML file inside a compressed license file.

To verify the contents of an NFM-P license file, for example, if you are unsure which file contains a specific license option or number of license points:

Note: A license file does not include an object that has a licensed quantity of zero.

1. Uncompress the license zip file.
2. View the contents of the contained XML file.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3. Close the file.

End of steps

21.38 How do I export the NFM-P license information or create a license point inventory?

21.38.1 Steps

1

Choose Help→License Information from the NFM-P main menu. The NSP Network Functions Manager - Packet License (Edit) form opens.

2

To export the form information to a file, perform the following steps.

1. Click Export License information to file. A Save as form opens.
2. Specify a name, location, and format for the file that is to contain the license information.
3. Click Save. The license information is saved in the specified file.

3

To create a license point inventory, perform the following steps.

Note: The license point inventory file is saved in XML format.

1. Click License Points Inventory. A Save as form opens.
2. Specify a name and location for the file that is to contain the license inventory.
3. Click Save. The license point inventory is saved in the specified file.

4

Close the NFM-P License (Edit) form.

End of steps

21.39 How do I update the NFM-P license in a standalone deployment?

21.39.1 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4

Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the NFM-P license zip file

The following prompt is displayed:

```
Detected an NFM-P license key. Do you want to proceed? (YES/no):
```

5

Enter the following:

YES ↵

The main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing NFM-P license key...
Original license key file has been backed up to
/opt/nsp/nfmp/server/timestamp/SAMLicense.zip
Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

6

Close the console window.

Verify new license information

7

Perform 21.37 “How do I view the NFM-P license information?” (p. 640) to verify the imported license information.

8

If a license parameter is incorrect, contact technical support for assistance.

END OF STEPS

21.40 How do I update the NFM-P license in a redundant deployment?

Note: The license files that you import to the primary and standby main servers must contain identical license quantity and option values.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: To reduce the risk of importing mismatched licenses, it is recommended that you obtain one license file that contains the system ID of each main server, and then import the same file on each main server.

Note: The primary and standby main server licenses must be synchronized to ensure correct NFM-P operation in the event of a server activity switch. The main servers compare license values after a system reconfiguration. If a difference is detected, the NFM-P raises an alarm that you can clear when the licenses are synchronized.

21.40.1 Steps

Update license on primary main server

1

Open a client GUI to monitor the NFM-P during the license update.

2

Log in to the primary main server station as the nsp user.

3

Open a console window.

4

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

5

Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the NFM-P license zip file

The following prompt is displayed:

```
Detected an NFM-P license key. Do you want to proceed? (YES/no):
```

6

Enter the following:

```
YES ↵
```

The primary main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing NFM-P license key...
Original license key file has been backed up to
/opt/nsp/nfmp/server/timestamp/SAMLicense.zip
Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: Importing the new license on the primary main server creates a license mismatch with the standby main server. As a result, the NFM-P raises an alarm that you can clear when the license import on each main server is complete.

7

Close the console window.

Update license on standby main server

8

Log in to the standby main server station as the nsp user.

9

Open a console window.

10

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

11

Enter the following:

```
bash$ ./nmsserver.bash import_license license_file ↵
```

where *license_file* is the absolute file path of the NFM-P license zip file

The following prompt is displayed:

```
Detected an NFM-P license key. Do you want to proceed? (YES/no):
```

12

Enter the following:

```
YES ↵
```

The standby main server reads the license file, copies the license file to a backup location, and displays the following status information:

```
Importing NFM-P license key...
Original license key file has been backed up to
/opt/nsp/nfmp/server/timestamp/SAMLicense.zip
Done.
```

where *timestamp* is a directory name in the following format: yyyy.mm.dd-hh.mm.ss

13

Enter the following to restart the standby main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

14

Enter the following:

```
bash$ ./nmsserver.bash appserver_status ↵
```

The server status is displayed; the server is fully initialized if the status is the following:

```
Application Server process is running.  See nms_status for more
detail.
```

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

15

Close the console window.

Verify new license information

16

Perform 21.37 “How do I view the NFM-P license information?” (p. 640) to verify the imported license information.

17

If a license parameter is incorrect, contact technical support.

18

After you verify that the license information is correct, clear the license mismatch alarm.

19

Close the GUI client, if it is no longer required.

END OF STEPS

21.41 How do I list the backed-up NFM-P license files?

21.41.1 Purpose

When you import an NFM-P license, the NFM-P creates a backup copy of the existing license file. The following steps describe how to list the NFM-P license files.

21.41.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4

Enter the following:

```
bash$ ./nmsserver.bash import_license ↵
```

The command lists the files, as shown below:

```
The following backed up license key files have been detected on the
system.
/opt/nsp/nfmp/server/timestamp1/SAMLicense.zip
/opt/nsp/nfmp/server/timestamp2/SAMLicense.zip
.
.
.
```

where *timestamp1* and *timestamp2* are directory names in the following format: yyyy.mm.dd-hh.mm.ss

5

Close the console window.

END OF STEPS

21.42 How do I change the default NFM-P license expiry notification date?

21.42.1 Purpose

The NFM-P raises a daily warning alarm as the expiry date of the NFM-P license approaches. By default, the first alarm is raised seven days before the expiry date. Perform the procedure to change the default license expiry notification date.

CAUTION

Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.42.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Locate the following tag in the nms-server.xml file:

```
<license
```

7

Edit the following line in the section to read:

```
timedLicenseExpiryCount="value"
```

where *value* is the number of days to be notified before the license expiry

8

Save and close the nms-server.xml file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```

The NFM-P puts the configuration change into effect.

10

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P network management configuration

21.43 How do I configure implicitly clearing alarm behavior for node reboots?

21.43.1 Purpose

CAUTION

Service Disruption

Modifying the NFM-P system configuration can have serious consequences that include service disruption.

Contact technical support before you attempt to modify the server configuration.

Use this procedure to specify that the alarm that is raised after an NE reboots is Implicitly Cleared for the following NEs: 7950 XRS, 7750 SR, 7705 SAR, 7705 SAR-H, 7450 ESS, 7250 IXR, and 7210 SAS.

Note: Enabling this function means that you may not be aware that an NE has rebooted.

21.43.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Add the following entry:

```
    <!--Configure the NFM-P to change "NodeRebooted" alarm to be
"Implicitly Cleared".

    ;The default value is "false". To change it as implicitly cleared
make it "true"
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
;
-->
<NodeRebootedAlarm implicitlyCleared="true"/>
```

7

Save and close the file.

8

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```

The NFM-P puts the configuration change into effect.

9

Close the console window.

END OF STEPS

21.44 How do I configure backup-file retention for deleted NEs?

21.44.1 Purpose

The NFM-P saves NE configuration backup files on each main server, and by default deletes the backup files of deleted NEs. To retain backups for deleted NEs, you can:

- Manage the disk space consumed by NE configuration backups using the following procedures (recommended):
  - 21.71 “How do I back up the NE configuration files?” (p. 689)
  - 21.72 “How do I restore the NE configuration files?” (p. 690)
- Disable the automatic deletion of deleted NE backup files, as described in the following procedure.

Note: If the NE is unmanaged, the backup files and other management data are always deleted.

CAUTION

Service Disruption

The procedure requires a restart of each main server, which causes a network management outage.

Perform the procedure only during a scheduled maintenance period.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each NFM-P main server station.

Note: You require nsp user privileges on each main server station.

21.44.2 Steps

1

Log in to the main server station as the nsp user.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor.

6

Locate the following lines:

```
;
; <nodeBackups removeBackupOnDelete="false"/>
;
```

7

Edit the lines to read as shown below:

```
;-->
<nodeBackups removeBackupOnDelete="value"/>
<!--;
```

where *value* is true, to enable backup file deletion, or false, to disable deletion

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Save and close the nms-server.xml file.

9

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

10

Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts.

Note: If you are restarting the primary main server in a redundant deployment, the network outage begins. The outage persists until the main server is fully initialized.

11

Close the console window.

END OF STEPS

21.45 How do I enable alarm reporting to identify duplicate NE system IP addresses?

21.45.1 Purpose

Enable the NFM-P to verify the uniqueness of NE system IP addresses.

When the verification is enabled, the NFM-P generates an alarm when an NE reports a system IP address that is in use by another NE.

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

21.45.2 Steps

1

Log in to the main server station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Open the nms-server.xml file using a plain-text editor.

5

Create a backup copy of the nms-server.xml file.

6

Locate the section that begins with the following XML tag:

```
<snmp
```

7

Insert the following before the section end, which is marked by a /> tag:

```
verifyNodeIdentity=”1"
```

Note: If the inserted text and end tag are on the same line, you must include a space between the text and the end tag.

8

Save and close the nms-server.xml file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```

The NFM-P puts the configuration change into effect.

10

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.46 How do I enable dynamic system IP address updates for 7705 SAR nodes?

21.46.1 Purpose

Allow the NFM-P to react automatically when the IP address of a 7705 SAR node changes, for example, after acquiring a new address via DHCP. 7705 SAR NEs are uniquely identified in the network by the System ID parameter. Before you attempt to enable dynamic system IP address updates, please consider the following:

- The system ID of each 7705 SAR must be unique, or the NFM-P may update SDPs to point to an incorrect NE. You can configure the system ID parameter through CLI.
- All 7705 SAR NEs in the network must be unmanaged before you attempt to perform the procedure.

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

21.46.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Open the nms-server.xml file using a plain-text editor.

5

Locate the following section:

```
<SARSysIPAddrChange
enabled="false"
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
ipRange="224.224.0.0"
prefix="24" />
```

6

Change `enabled="false"`.to `enabled="true"`.

7

Save and close the nms-server.xml file.

8

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```

The NFM-P puts the configuration change into effect.

9

Close the console window.

END OF STEPS

21.47 How do I enable LSP on-demand resynchronization?

21.47.1 Purpose

By default, LSP on-demand resynchronization is disabled. When you enable LSP on-demand resynchronization, the NFM-P scheduled resynchronization is then disabled for some LSP objects. See “LSP on-demand resynchronization” in the *NSP NFM-P Classic Management User Guide* for information about which LSP objects do not support on-demand resynchronization.

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

21.47.2 Steps

1

Log in to the main server station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory .

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor.

6

Locate the following line:

```
lspOnDemand overrideEnabled="false" />
```

7

Change "`false`" to "`true`".

8

Save and close the nms-server.xml file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↲
```

The NFM-P puts the configuration change into effect.

10

Close the console window.

END OF STEPS

21.48 How do I enable debug configuration file reloading on an NE for mirror services?

21.48.1 Purpose

Ensure that the managed NEs reload the debug configuration file after an NE restart. This ensures that the mirror services in the managed network resume operation after a reboot or a CPM activity switch on the NE that hosts the mirror service. By default, debug configuration file reloading is disabled.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

CAUTION

Service Disruption

The procedure requires a restart of each main server, which is service-affecting.

Ensure that you perform the procedure only during a scheduled maintenance window.

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

21.48.2 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Open the nms-server.xml file using a plain-text editor.

5

Locate the section that begins with the following XML tag:

```
<serviceMirror
```

6

Specify the NE location of the debug configuration file. For example:

```
<serviceMirror
debugFilename="filename"
reloadDelay="delay"
/>
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

where

filename is the absolute file path of the debug log on the NE, for example, cf3:/ServiceMirror.dbg

delay is the time, in seconds, to wait before a reload request is sent

7

Save and close the nms-server.xml file.

8

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

9

Enter the following to restart the main server:

```
bash$ ./nmsserver.bash force_restart ↵
```

The main server restarts.

10

Close the console window.

END OF STEPS

21.49 How do I configure throttle rates for subscriber trap events?

21.49.1 Purpose

Configure throttle rates for residential subscriber create and delete event traps on a 7750 SR. The throttle rate specifies the number of events that are received in a specified period before the NE stops sending individual traps.

21.49.2 Steps

1

On the equipment tree, right-click on the NE for which you want to configure trap event throttle rates and choose Properties. The Network Element (Edit) form opens.

2

Click Event Throttling. The ESM Trap Throttle form opens.

3

Disable the Default check box and configure the required parameters.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Click Execute. The Detailed Status/Error message field displays status information about the throttle rate change.

5

Close the Network Element (Edit) form.

END OF STEPS

21.50 How do I configure the windowing trap delayer option for subscriber table resyncs?

21.50.1 Purpose

Configure the windowing trap delayer option to provide an enhanced method to resynchronize the subscriber table in the event that an NE drops a trap.

Configurable hold-off options prevent subscriber table resyncs for a minimum specified duration after a trap drop is received from an NE, and until a specified period has elapsed with no additional trap drops. Additionally, a maximum hold-off time is specified to prevent excessive periods during which the NFM-P is not synchronized with the NE. The windowing trap delayer configuration reduces the number of subscriber table resync events while attempting to maintain synchronization with the NE.

Note: The windowing trap delayer option affects only tmnxTrapDropped traps associated with tmnxSubscriberCreated, tmnxSubscriberDeleted or tmnxSubscriberRenamed traps. When the windowing trap delayer option is disabled, tmnxTrapDropped traps are delayed using the default trap delay function.

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

21.50.2 Steps

1

Log in to the main server station as the nsp user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor.

6

Locate the section that begins with the following XML tag:

```
<snmp
```

7

Add the following to the section:

Note: The checkInterval value must be less than the windowLength value, which must be less than the maxHoldOff value.

```
<windowingTrapDelayer
enabled="true"
checkInterval="interval"
windowLength="duration"
maxHoldOff="wait" />
```

where

interval is the minimum time, in seconds, during which subscriber table resynchronzation is prevented; the range is 5 to 30, and the default is 10

duration is the time, in seconds, during which no additional trap drops can be received before subscriber table resyncs are allowed; the range is 5 to 60, and the default is 30

wait is the maximum hold-off time, in seconds, after which subscriber table resynchronization is allowed; the range is 5 to 1800; the default is 60

8

Save and close the nms-server.xml file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The NFM-P puts the configuration change into effect.

10

Close the console window.

END OF STEPS

21.51 How do I create a default SNMPv2 OmniSwitch user?



CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

Note: You must perform the procedure on each main server in the NFM-P system.

Note: In a redundant system, you must perform the procedure on the standby main server station first.

21.51.1 Steps

1

Log in to the main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

4

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor.

6

Locate the section that begins with following XML tag:

```
<snmp
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Insert the following before the section end, which is marked by a /> tag:

```
snmpV2UserName="username"
```

where *username* is a user name that is configured on the OmniSwitch

Note: If the inserted text and end tag are on the same line, you must include a space between the text and the end tag.

The section now reads as follows:

```
<snmp
ip="IPv4_address"
port="nnnnn"
ipv6="IPv6_address"
msgMaxSize="nnnn"
natEnabled="value"
trapLogId="nn"
snmpV2UserName="username" >
```

8

Save and close the nms-server.xml file.

9

On a standalone main server, or the primary main server in a redundant system, enter the following:

```
bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
```

The NFM-P puts the configuration change into effect.

10

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Setting NFM-P OLC states

21.52 What is an OLC state?

21.52.1 Description

Performing a maintenance operation on an NE can generate a considerable number of NFM-P alarms that are not of interest to an operator. You can configure the OLC state of a service or equipment object to specify whether the object is in service or in maintenance mode. During a subsequent maintenance operation, you can filter alarms using the OLC state as a criterion in order to display only the alarms of interest.

Note: The NFM-P raises alarms against service and equipment objects regardless of the OLC state, which is not deployed to NEs.

You can set the OLC state on the following equipment and service objects:

- network elements
- power supply trays
- card slots
- daughter cards
- ports
- LAGs
- composite services
- services
- sites
- SAPs

Note: A shelf OLC state is inherited from the parent NE, and is not configurable.

On equipment and service properties forms, you can configure the NFM-P to change the OLC state of an object after a specified time, depending on the current OLC state. In a device discovery rule, you can configure the default OLC state for NEs, and can specify that the current OLC state reverts when the NE discovery is complete. You can also specify that the NFM-P raise an informational alarm about an object OLC state reverting to the opposite state. See the *NSP NFM-P Classic Management User Guide* for information about device discovery rules and OLC states.

21.52.2 Setting the OLC state

CAUTION

Service Disruption

Changing the OLC state of an object also changes the OLC state of child objects that are not locked in maintenance mode, and may affect NFM-P system performance.

Ensure that you change the OLC state of an object that has many child objects only during a period of low NFM-P activity, such as during a scheduled maintenance period.

Note: An OLC state change operation may take several minutes to complete, depending on the number of objects that the state change affects.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

A child object inherits the OLC state of the parent object. However, you can lock the OLC state of a child object in maintenance mode to prevent the inheritance in the event that the parent OLC state changes. Locking the OLC state of an object also locks the OLC state of each child object.

You can specify a global default OLC state for discovered services; see 21.11 “How do I set the NFM-P system preferences?” (p. 603).

During a shutdown or turn-up operation, the OLC state of the parent object overwrites the OLC state of each child object, unless the OLC state of a child object is locked in maintenance mode. The NFM-P Task Manager logs the OLC state change of an object, but does not log the OLC state changes of the child objects.

Note: When an OLC state change affects a large number of objects, alarms raised against affected objects before the state change is propagated show the previous OLC state. Also, if an operator shuts down an equipment or service object via CLI, the associated NE trap handling for the child objects requires additional processing which can cause the same propagation delay and OLC state misrepresentation in alarms.

21.52.3 Functional description

When the OLC state of an NE is set to maintenance mode, all child objects such as access interfaces, card slots, daughter cards, and ports are set to maintenance mode, as is each service site on the NE.

When the OLC state of a composite service or service is set to the maintenance mode, the following child objects are affected:

- service sites
- L2 and L3 SAPs
- SDP bindings

When the OLC state of a composite service or services changes to in service, the OLC states of the associated sites and SAPs do not change if the host equipment objects are in maintenance mode.

The OLC state of an object must be in service before you can change the OLC state of a child object. You can change the OLC state of a parent object regardless of the OLC state of a child object, but if a child object has more than one parent object and the OLC state of one parent is set to maintenance, the child object is set to maintenance. You cannot change the OLC state of an object when a parent OLC state is set to maintenance.

You can configure the default OLC state for objects that become administratively down from the OLC tab of the System Preferences form; see 21.11 “How do I set the NFM-P system preferences?” (p. 603).

You must add the OLC state property to manually created service templates, as described in 21.59 “How do I add the OLC state property to a manually created service template?” (p. 668) .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.53 How do I display equipment or service OLC states?

21.53.1 Steps

1

Choose Administration→OLC from the NFM-P main menu. The OLC form opens.

2

Choose a service or network object from the drop-down menu and click Search. A list of objects is displayed.

3

View the Current OLC State and Lock OLC State values.

4

Close the OLC form.

END OF STEPS

21.54 How do I display the OLC state change schedules?

21.54.1 Steps

1

Choose Administration→OLC from the NFM-P main menu. The OLC form opens.

2

Click on the Schedules tab. A list of scheduled OLC state changes is displayed.

3

View the following information:

- object ID and name
- current OLC state
- OLC state to which the object reverts at the scheduled time
- time when the OLC state changes

4

As required, select an entry and click Properties to view more information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Close the open forms.

END OF STEPS

21.55 How do I change the OLC state of one or more objects?



CAUTION

Service Disruption

Changing the OLC state of an object also changes the OLC state of child objects that are not locked in maintenance mode, and may affect NFM-P system performance.

Ensure that you change the OLC state of an object that has many child objects only during a period of low NFM-P activity, such as during a scheduled maintenance period.

Note: You can change the OLC state of multiple services at once only if the services are of the same type.

Note: An OLC state change operation may take several minutes to complete, depending on the number of objects that the state change affects.

21.55.1 Steps

1

Perform one of the following.

a. Use the OLC form.
   1. Choose Administration→OLC from the NFM-P main menu. The OLC form opens.
   2. Choose a service or network object type from the drop-down menu and click Search. A list of objects is displayed.
   3. Select one or more entries and click OLC State→Maintenance or OLC State→In Service.

b. Use an object properties form.
   1. Open the object properties form of one object, or the multi-instance properties form of multiple objects. A properties form opens.
   2. Configure the Current OLC State parameter.

The OLC state of each selected object changes.

2

Save the changes and close the open forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.56 How do I lock the OLC state?

21.56.1 Purpose

You can lock the OLC state of a child object that is in maintenance mode to prevent the OLC state from changing in the event that the parent object OLC state changes to In Service. Locking the OLC state of an object disables any associated scheduled OLC state change. Also, when the OLC state of an object is locked, you cannot configure the Revert OLC State parameter of the object.

Note: You can lock the OLC state of multiple objects at once.

21.56.2 Steps

1

Choose Administration→OLC from the NFM-P main menu. The OLC form opens.

2

Choose a service or network object type from the drop-down menu and click Search. A list of objects is displayed.

3

Select one or more entries and click Properties. The object or multi-instance properties form opens.

4

Configure the Lock OLC State parameter.

Note: You can lock the OLC state only when the Current OLC State parameter is set to Maintenance.

Note: If all selected objects have an OLC state of Maintenance and one or more objects is locked in maintenance mode, the Lock OLC State parameter is selected and dimmed, but is configurable.

5

Save the changes and close the OLC form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.57 How do I schedule an OLC state change?

CAUTION

Service Disruption

Changing the OLC state of an object also changes the OLC state of child objects that are not locked in maintenance mode, and may affect NFM-P system performance.

Ensure that you schedule the OLC state change of an object that has many child objects to occur during a period of low NFM-P activity, such as during a scheduled maintenance period.

21.57.1 Steps

1

Choose Administration→OLC from the NFM-P main menu. The OLC form opens.

2

Choose a service or network object type from the drop-down menu and click Search. A list of objects is displayed.

3

Select one or more entries and click Properties. The object properties or multi-instance properties form opens.

4

Configure the Revert OLC State parameter. If you set the parameter to Custom, use the calendar tool to specify a time and date at which the OLC state is to change.

Note: If multiple objects are selected, a schedule is created for each object. Also, the OLC State Will Revert To and Revert OLC Time indicators are not shown on multi-instance properties forms; you must open the properties form for one object to view the indicators.

5

Save the changes and close the OLC form.

END OF STEPS

21.58 How do I change the OLC state assigned to one or more alarms?

21.58.1 Steps

1

If required, create an alarm filter.

1. Click on the filter icon in the Alarm Window. A filter form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Choose Assigned OLC State from the Attribute drop-down menu.
3. Configure the filter, as required. See the *NSP NFM-P Classic Management User Guide* for information about creating alarm filters.

2

Select one or more alarms in the alarm list.

3

Right-click on the selected alarms and choose Assign OLC State. The OLC State Assignment form opens.

4

Configure the Assigned OLC State parameter.

5

Save the changes and close the OLC State Assignment form.

END OF STEPS

21.59 How do I add the OLC state property to a manually created service template?

21.59.1 Purpose

You cannot configure the OLC state property of a service object during object creation. The OLC state property is automatically included in an NFM-P-created service template, but not in a manually created service template.

21.59.2 Steps

1

Open the GUI builder, as described in the *NSP NFM-P Scripts and Templates Developer Guide*.

2

Create a combo box component and enter olcState as the Name attribute value.

3

Enter the following as the List attribute values:

- inService
- maintenance

4

Enter one of the following as the Default attribute value:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- inService
- maintenance

5

Save the changes and close the open forms.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P platform modification and replacement

21.60 What is platform modification?

21.60.1 Platform modification



CAUTION

Service Disruption

To avoid a network management outage, it is strongly recommended that you contact technical support before you attempt to modify an NFM-P component platform.

An NFM-P component may require reconfiguration or another type of action in response to a change in the available platform resources.

After you reconfigure the platform of a main server, main database, or auxiliary server station, you must ensure that the station reboots successfully before you restart the NFM-P software on the station.

Basic platform modifications include:

- Number of CPUs
- Amount of RAM
- NIC type
- OS patch or upgrade
- IP-address or hostname change;see the following, as required:
  - 21.63 “How do I change the IP address or hostname of an NFM-P component?” (p. 675)
  - 20.12 “How do I change the auxiliary database external IP addresses?” (p. 542)

Some components require specific configuration as part of a platform modification; see the following, as required:

- any component, before increasing LVM disk space—21.61 “How do I test NFM-P disk performance?” (p. 671)
- main database, after an OS patch or upgrade—21.62 “How do I relink the Oracle executable files?” (p. 674)

21.60.2 Platform replacement

In the event that an NFM-P component station fails and cannot be recovered, you must re-install the component on a replacement station that has the same platform specifications as the original station. If you want to use a station with different specifications, you must contact technical support to develop an approved hardware migration strategy.

After you replace the platform of an NFM-P component, you must ensure that the newly installed component on the replacement station retains all functions and customized properties of the original component.

Some components, such as main servers, may have custom settings in configuration files. In order to restore the original server functions, you must restore the custom settings. Each NFM-P

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

procedure that describes modifying parameters in configuration files includes a step to back up the current configuration to a secure location. After a replacement component is installed, and before the component initializes, you must use the backup files to replace the newly installed files. Contact technical support for more information.

Multi-vendor driver restoration

MV driver files are installed on a main server after the main server installation. If your NFM-P system manages devices using MV drivers, and the main server fails, you must re-install the drivers on the replacement main server.

Note: Until the MV drivers are installed on the new main server, any devices managed using the drivers are in the Suspended state, and the driver status indicates that the driver file is absent from the main server file system.

See the *NSP NFM-P Classic Management User Guide* for driver installation information.

21.61 How do I test NFM-P disk performance?

21.61.1 Purpose

Perform this procedure to check the disk performance on an NFM-P component station.

The disk performance of an NFM-P component affects overall system performance, and must meet or exceed the minimum specifications in the response to the NFM-P Platform Sizing Request for your system. See the *NSP NFM-P Release Description* for information about submitting a Platform Sizing Request.

Also, before you add capacity to a disk or partition on an NFM-P component, for example, using LVM, you must ensure that the disk throughput and latency values remain within tolerance, which is defined as being within 10% of the current values.

CAUTION

Service Disruption

Checking NFM-P disk performance requires a shutdown of one or more NFM-P components, which is service-affecting.

Perform the procedure only during a scheduled maintenance period.

21.61.2 Steps

1

Perform one of the following, depending on the type of component for which you need to check performance:

a. Shut down a main server.
   1. Log in to the main server station as the nsp user.
   2. Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3. Navigate to the /opt/nsp/nfmp/server/nms/bin directory.
4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

5. Enter the following to display the server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

b. Shut down an auxiliary server.

1. Log in to the auxiliary server station as the nsp user.
2. Open a console window.
3. Navigate to the /opt/nsp/nfmp/auxserver/nms/bin directory.
4. Enter the following:

   ```
   bash$ ./auxnmsserver.bash auxstop ↲
   ```

5. Enter the following to display the auxiliary server status:

   ```
   bash$ ./auxnmsserver.bash auxappserver_status ↲
   ```

   The command returns a status message.
6. The server is fully stopped when the following is displayed:

   ```
   Auxiliary Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is stopped.

c. Shut down a main database.

1. Log in to the main database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↲
   ```

4. Enter the following to stop the main database:

   ```
   # systemctl stop nfmp-main-db.service ↲
   ```

d. Shut down an auxiliary database; perform 20.4 “How do I stop an auxiliary database cluster?” (p. 525).

2

If you are performing the test on a main or auxiliary server station, enter the following to switch to the root user:

```
bash$ su - ↲
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Perform one of the following.

a. On a main server station, enter the following:

```
# /opt/nsp/nfmp/server/nms/bin/unsupported/IOTest/NSP_IOTest.pl -d target ↵
```

where *target* is the disk partition to test

b. On an auxiliary server station, enter the following:

```
# /opt/nsp/nfmp/auxserver/nms/bin/unsupported/IOTest/NSP_IOTest.pl -d target ↵
```

where *target* is the disk partition to test

c. On a main database station, enter the following:

```
# /opt/nsp/nfmp/db/install/tools/unsupported/IOTest/NSP_IOTest.pl -d target ↵
```

where *target* is the disk partition to test

4

Record the utility output.

5

If you are performing the test as a pre-upgrade task specified in the *NSP Installation and Upgrade Guide*, or as a general performance check, perform the following steps.

1. Compare the following recorded values with the values specified for your system:
   - main server, main database, or auxiliary server—Read, Write, and Latency
   - NSP auxiliary database—Read, Write, Rewrite, and %IO Wait
2. If the values do not meet the minimum specifications, contact the NFM-P Platform Team through your account representative.
3. Go to Step 8.

6

If you are adding capacity to a disk or partition, perform the following steps.

1. Add the required capacity to the disk or partition.
2. Repeat Step 3 and Step 4 as required.
3. Compare the following values from before and after the capacity increase:
   - main server, main database, or auxiliary server—Read, Write, and Latency
   - auxiliary database—Read, Write, Rewrite, and %IO Wait
4. If the values differ by more than 10%, contact the NFM-P Platform Team through your account representative.

7

Restart the component that you shut down and tested in step 1. Perform one of the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

a. Restart a main server.
   1. Enter the following to switch back to the NSP user:
      ```
      # exit ↵
      ```
   2. On a main server station, navigate to the /opt/nsp/nfmp/server/nms/bin directory.
   3. Enter the following:
      ```
      bash$ ./nmsserver.bash start ↵
      ```
      The main server starts.

b. Restart an auxiliary server.
   1. Enter the following to switch back to the NSP user:
      ```
      # exit ↵
      ```
   2. On an auxiliary server station, navigate to the /opt/nsp/nfmp/auxserver/nms/bin directory.
   3. Enter the following:
      ```
      bash$ ./auxnmsserver.bash auxstart ↵
      ```

c. Restart a main database.
   1. Enter the following to start the Oracle proxy:
      ```
      # systemctl start nfmp-oracle-proxy.service ↵
      ```
   2. Enter the following to start the main database:
      ```
      # systemctl start nfmp-main-db.service ↵
      ```

d. Restart an auxiliary database; perform 20.3 “How do I start an auxiliary database cluster?” (p. 523).

8

Close the console windows, as required.

END OF STEPS

21.62 How do I relink the Oracle executable files?

21.62.1 Purpose

Perform this procedure to relink the Oracle executable files on a main database station after you apply an OS patch, or after an OS upgrade.

CAUTION

Service Disruption

This procedure requires a restart of the main database, which is service-affecting.

You must perform the procedure only during a scheduled maintenance period.

Note: You require root user privileges on the main database station.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.62.2 Steps

1

Log in as the root user on the main database station.

2

Open a console window.

3

Enter the following:

```
# chmod 755 /usr/bin/make ↵
```

4

Enter the following:

```
# /opt/nsp/nfmp/db/install/config/samdb/relinkOracle.sh ↵
```

The script relinks the Oracle executable files.

5

When the script execution is complete, enter the following to reboot the database station:

```
# systemctl reboot ↵
```

The station reboots, and the main database initializes.

6

After the reboot, enter the following:

```
# chmod 750 /usr/bin/make ↵
```

7

Close the console window.

END OF STEPS

21.63 How do I change the IP address or hostname of an NFM-P component?

21.63.1 Purpose

Changing the IP address or hostname of one or more NFM-P components in a standalone or redundant system may be required, for example, when the management network topology changes.

The requirements of such an operation depend on the management network topology and other considerations, so must be co-ordinated and performed only under the guidance of technical support.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



CAUTION

Service Disruption

Changing an IP address or hostname in an NFM-P system is a complex operation that requires careful planning and organization, and depending on the type of change required, may involve a brief network management outage.

Do not attempt to modify the network configuration of an NFM-P component without assistance from technical support.

21.63.2 Steps

1

Collect the following information:

- hostname of each main server, main database, auxiliary server, and client delegate server station
- current IP address of each interface that is used by the main servers, main databases, auxiliary servers, NSP auxiliary databases, and client delegate servers
- hostname and IP address of each NSP component that the NFM-P communicates with
- configuration information for mechanisms in the management network that affect addressing, such as NAT
- new IP addresses and hostnames of the components

2

Contact technical support to schedule a maintenance period for the network configuration change.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

NFM-P maintenance

21.64 What is NFM-P system maintenance?

21.64.1 Introduction

The implementation of a regular maintenance schedule is recommended in order to:

- prevent downtime caused by software, platform, or network failure
- enable maximum system performance

NFM-P system maintenance begins with the establishment of base measures against which to evaluate the system functionality and correct any performance or connectivity issues.

NFM-P OLC states

You can put NEs in maintenance mode using OLC states, as described in “Setting NFM-P OLC states” (p. 662).

21.64.2 NFM-P base measures

Maintenance base measures can be used by NOC operations or engineering staff who are responsible for maintenance issues to evaluate the activity and performance of network components, for example, client GUI response times when listing equipment.

The data from a series of base measures can be used, over time, to track performance trends. For example, if there are reports that client GUI response times for listing equipment degrades over time, you can use the base measures to determine how much performance has degraded. The procedures in this guide can help narrow the search for the cause of performance degradation.

It is recommended to do the following:

- Determine the types of base measures required for your network.
- Record base-measure data.
- Regularly collect system information and compare the information with the base measure data.

This section provides base measure information for:

- platform—to ensure system sizes are tracked
- performance and scalability—to categorize system limitations as a baseline against NMS response times
- inventory counts—to generate inventory lists for storage and post-processing
- reachability—to ensure that customer services are available

21.64.3 Establishing base measures

Base measures can be affected by issues that are beyond the scope of this guide, including:

- network topology design
- NOC or operations area LAN design

The NFM-P service test manager (STM) provides the ability to group OAM diagnostic tests into test suites that you can run as scheduled tasks. You can customize a test suite to your network topology

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

and execute the test suite to establish baseline performance information. You can retain the test suite, modify it to accommodate network topology changes, and execute the test suite to establish new base measures as required. Scheduled execution of the test suite and regular review of the results may reveal deviations from the baseline. See the *NSP NFM-P Classic Management User Guide* for information about using the STM and creating scheduled tasks.

21.64.4 Platform base measures

You can use platform base measures to:

- record the details of the platform configuration
- track network-specific growth to provide a delta for performance measures, for example, how long it takes to list 1000 ports on the current station compared to 10 000 ports on the same station, or on a smaller or larger station

Table 21-4 Platform base data

Component	Platform information
Main server 1	RAM: CPU (quantity, type, speed): OS version and patch level:
Main database 1	RAM: CPU (quantity, type, speed): OS version and patch level:
Main server 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slices:
Main database 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Database disk file systems: Disk slice sizes:
Auxiliary server 1	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:
Auxiliary server 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-4 Platform base data (continued)

Component	Platform information
Auxiliary server 1	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:
Auxiliary server 2	RAM: CPU (quantity, type, speed): OS version and patch level: Swap space: Disk slice sizes:
Client delegate server	OS type, version, patch level: RAM: CPU: Disk space: Monitor: Graphics card:
Single-user GUI client	OS type, version, patch level: RAM: CPU: Disk space: Monitor: Graphics card:
Single-user GUI client	RAM: CPU: OS type, version, patch level: Disk space: Monitor: Graphics card:

21.64.5 Inventory base measures

You can use inventory base measures to:

- create lists of network objects for future processing
- track network-specific growth to provide a delta for any performance measures, for example, how long it takes 5 versus 15 client GUIs to list 1000 ports

Use the following sequence to create inventory base measures, for example, for access ports. You can modify the sequence to create additional inventory base measures for other objects.

1. Determine the type of object data for which you need to create inventory records, for example, access ports.
2. List the ports of all managed network devices using the client GUI manage equipment window or create an XML API request to generate the list.
3. Format the inventory for future processing, based on your inventory processing requirements.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4. Generate the inventory data, using the same listing and filtering criteria, on a weekly or monthly basis, as necessary to track changes to the network.

   When new devices are added to the network on a regular basis, increase the inventory frequency.

5. Use the generated list to record the current inventory of network objects and as a baseline measure of performance.

   For example, baseline the time required to generate a client GUI list of 1000 access ports.

   When an access port list is later generated, record the time required to generate the list using 2000 ports. Ideally, it takes twice as long to list twice as many ports; if the ratio of listing time to number of ports is highly nonlinear, there may be scalability issues that require investigation.

21.64.6 Performance and scalability base measures

You can use the following performance and scalability base measures to:

- record the system limit numbers and compare to the measurement data collected in your network
- track network-specific growth to provide a delta for any performance measures on similarly-sized platforms, for example, how long it takes to discover 10 new devices versus 20 new devices
- quantify user perceptions of performance

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table 21-5 Scalability base measures

Type of base measure	System limits	Expected response time	Network base measure response time	Additional information
Total devices managed	See the appropriate *NSP NFM-P Release Description* and *NSP Planning Guide* for information about release-specific system limits.	The client GUI is operational *XX* seconds after launching.		The time to open icons in the Equipment navigation tree increases depending on the number of configured MDAs.
Total services		• XML API configuration of 300 VLL services in *X* min • XML API configuration of 100 VPLS services with 3 sites and one SAP in 5 min		The complexity of the service configuration affects response time. For example, adding additional SAPs to a VPLS increases provisioning time.
Outstanding alarms		The client GUI is able to retrieve and display *XX* 000 alarms in the dynamic alarm list during startup.		—
Client GUIs for each server		—		Open a configuration form using the client GUI in X amount of time. Measure X against a constant platform size over time
Device discovery		Discover one additional device with an IP address in the X.X.X.1 to 255 range in less than 1 min.		—

21.64.7 Performance base measures

For networks, commonly available tools such as ping, which measures round trip time using ICMP, can be used to determine quantities such as packet loss and round trip delay. See the ping command information in this guide, and the *NSP Troubleshooting Guide*, for more information about performing the commands.

- Packet loss is defined as the fraction of packets sent from a measurement agent to a test point for which the measurement agent does not receive an acknowledgement from the test point. Acknowledgements that do not arrive within a predefined round trip delay at the measurement agent are considered lost.
- Round trip delay is defined as the interval between the time a measurement agent sends a packet to a test point and the time it receives acknowledgement that the packet was received by the test point.

You can baseline the packet loss results and round trip delay times for specific NMS LAN and network scenarios. Record those results for future baselines against regularly run packet loss and round trip delay tests.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.64.8 Reachability base measures

System reachability is important in business-critical systems. Service reachability components are:

- Can the customer reach the service? (reachability)
- If so, is the service available for customer use? (service availability)
- If not, how frequently and how long do service outages last? (service outage duration)

The types of measures and baselines necessary to ensure reachability and availability are network-dependent, and vary depending on the topology of the network, the networking technologies used to move data, and the types of equipment used.

NE reachability

A test point is reachable from a testing measurement agent when the agent can send packets to the test point and receive a response from the test point that the packet was received. The ping test and the OAM diagnostics using the NFM-P or device CLI can test reachability. Record the test results to create a measurement baseline.

These tests can be performed when you troubleshoot a customer service, or when you perform SLA tests before you enable a customer service.

Service availability

The network between a measurement agent and a test point is considered available at a given time when the measured packet loss rate and the round trip delays are both below predefined thresholds. The threshold values are dependent on network topology. The ping test and the OAM diagnostics using the NFM-P or CLI to a device can test service availability. Record the test results to create a measurement baseline.

Service outage duration

The duration of an outage is defined as the difference between the time a service becomes unavailable and the time it is restored. Time between outages is defined as the difference between the start times of two consecutive outages. Troubleshooters that resolve customer problems, or the data generated to resolve SLAs, can provide the baseline metrics to measure outages, and the time between outages. Record the information to create a measurement baseline.

21.65 How do I back up the main database?

21.65.1 Overview

It is strongly recommended that you frequently back up the main database to prevent network data loss in the event of a failure. Other reasons for performing a database backup include the following:

- To move a database from one station to another
- To set aside a clean copy of the database before performing a system upgrade
- As a preventive measure before making a major change to the network

You can use the NFM-P client GUI or a CLI script to perform an immediate backup, and can use the GUI to schedule regular backups. See Chapter 22, “Classic management database administration” for information.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

It is recommended that you perform a daily backup of the file system on each NFM-P station to enable the component restoration in the event of a catastrophic failure.

21.66 How do I collect and store NFM-P log and configuration files?

21.66.1 Overview

When an NFM-P system runs for long periods with significant activity, the number of generated log files can consume a large amount of disk space. You must ensure that the contents of the NFM-P log directories are backed up on a regular basis to maintain a system activity record and to save disk space. It is also recommended that you back up the NFM-P configuration files

Note: You must contact technical support to modify the NFM-P log storage parameters.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Daily maintenance

21.67 How do I check the main database performance?

21.67.1 Steps

Monitor device synchronization to confirm that the main database information is maintaining synchronization with the NE configuration information.

1

Check for deployment failures. Deployment failures indicate that communication with a managed NE is failing.

1. Choose Administration→NE Maintenance→Deployment from the NFM-P main menu. The Deployment form opens.
2. Click Search to display the latest information.

   When no failed deployments are listed, deployment problems are not causing a synchronization issue.
3. If deployments are listed, view the state of a deployment in the State column. The possible deployment states include:
   - Canceled
   - Deployed
   - Failed (Configuration). Failure occurred because the configuration could not be applied to the specified objects.
   - Failed (Internal Error). Failure occurred due to general error conditions. The state is intended for all other possible errors.
   - Failed (Partial). Failure occurred at deployment and some of the configuration may have been sent to the network.
   - Failed (Resource Unavailable). Failure occurred because one of the resources required to apply the configuration is not in the main database.
   - Not Deployed
   - Pending
   - Postponed
4. Identify the source of the deployment problem. For example, for a Failed configuration state, ensure the configuration was performed correctly on the client GUI.

2

If you determine that there is a deployment problem and the problem is unrelated to the NFM-P or device configuration, use your company IT policies to check the LAN for connectivity and transmission problems, such as collisions and CRC errors.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.68 How do I back up the NFM-P log and configuration files?

21.68.1 Process

Perform this procedure to save a copy of the NFM-P installation log and configuration files for later analysis in the event of a failure.

Note: During a system restart, NFM-P log files are backed up to directories that are named using a timestamp. A component that runs for a long time can generate multiple log files. Before you restart an NFM-P component, ensure that there is sufficient disk space to store the backed-up log files.

21.68.2 Steps

1

Copy the following files from the /tmp directory on a RHEL station, or from the *installation_directory*\client directory on a Windows client station:

- NFM-P_*component*_stderr.txt
- NFM-P_*component*_stdout.txt.

where *component* is the NFM-P component type, for example, Main_Server, Main_Database, or Client

2

Copy the following file from each GUI client station; rename each file to indicate the client station from which it is copied:

- *installation_directory*/nms/config/nms-client.xml

3

Copy the following file from each main database station:

- /opt/nsp/nfmp/db/install/config/dbconfig.properties

4

Copy the following files from each main server station.

- /opt/nsp/nfmp/server/nms/config/nms-server.xml
- all log files in the /opt/nsp/nfmp/server/nms/log/server directory
- all log files in the /opt/nsp/nfmp/server/nms/log/jmsserver directory

When an NFM-P log file reaches a predetermined size, the NFM-P closes, compresses, and renames the file by including a sequence number and a timestamp. The following is an example of the filename format:

EmsServer.*#.timestamp*.log

where

is a sequence number; the sequence begins at 0

timestamp is the log closure time, in the following format: YYYY-MM-DD_hh-mm-ss

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Copy the following file from each auxiliary server station:

- /opt/nsp/nfmp/auxserver/nms/config/nms-auxserver.xml

6

Transfer the files to a secure location that is not in the network management domain.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Weekly maintenance

21.69 How do I back up and restore NE configuration files?

21.69.1 Description

The NFM-P stores NE configuration files on a main server file system. The following procedures describe how to create a backup archive of all NE configuration files on a main server, and how to restore an NE backup archive, for example, after a main server disk failure.

21.69.2 Device backups

The NFM-P backs up device files that include the following, depending on the device type and configuration:

Note: NE backup is not supported for NEs in model-driven mode. NEs in model-driven mode must be excluded from backup/restore policies.

- boot options file, or BOF
- primary-config file specified in the BOF
- port index file
- SAP index file
- LI configuration file
- NE license file
- debug file
- security certificate files

An NFM-P user requires the following to schedule device backups:

- an assigned Administrator scope of command role, or a scope of command role with write access to the mediation package
- FTP access on the device
- devices that have the BOF persist parameter enabled

21.70 How do I check the NE scheduled backup status?

21.70.1 Steps

1

Choose Administration→NE Maintenance→Backup/Restore from the NFM-P main menu. The Backup/Restore form opens.

2

Click on the Backup/Restore Status tab. The managed NEs are listed and backup and restore status information is displayed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Select an NE and click Properties. The NE Backup/Restore Status form opens.

4

View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.

5

Ensure that the NE configuration file and the associated index file are saved on the NE and available for backup. Click on the Configuration Saves tab, and ensure that the Config Save State indicator reads Success.

See the appropriate device documentation for more information.

6

Click on the Backups tab to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.

7

Click on the Faults tab to view additional troubleshooting information.

8

Close the NE Backup/Restore Status form.

9

Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab.

10

Select the backup policy for the NE and click Properties. The Backup Policy (Edit) form opens.

11

Ensure that the policy is assigned to the NE.

1. Click on the Backup/Restore Policy Assignment tab. The Backup Policy - Filter form opens.
2. Configure the policy filter criteria and click OK. The Backup Policy - Filter form closes.
3. Move the NE to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow.
4. Save your changes and close the form.

12

Click on the General tab on the Backup Policy (Edit) form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

13

Select the Enable Backup check box.

14

Modify the other parameters, if required.

15

Save your changes and close the form.

END OF STEPS

21.71 How do I back up the NE configuration files?

Note: Depending on the size and number of NE configuration files, a backup operation may take considerable time.

21.71.1 Steps

1

Log in to the standalone main server station, or the primary main server station in a redundant deployment, as the nsp user.

2

Open a console window.

3

Enter the following:

```
bash$ mkdir /opt/nsp/nfmp/nebackup/backup ↵
```

4

Enter the following:

Note: If you intend to copy and paste the command from this step into the console window, ensure that you remove the line breaks from the command text before you paste the text.

```
bash$ tar cf - --exclude='backup' /opt/nsp/nfmp/nebackup/ | gzip -c
>/opt/nsp/nfmp/nebackup/backup/nebackup_`date +"%Y-%m-%d-%H-%M"`.tgz ↵
```

A compressed archive file named *YYYY-MM-DD-hh-mm*.tgz is created in the /opt/nsp/nfmp/nebackup/backup directory, where *YYYY-MM-DD-hh-mm* is the file creation time.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

When the backup operation is complete, copy the file to a secure station that is not part of the NFM-P system. If you lack access to such a station, and the NFM-P system is redundant, copy the file to the standby main server station.

6

Close the console window.

END OF STEPS

21.72 How do I restore the NE configuration files?

Note: Depending on the size and number of NE configuration files, a restore operation may take considerable time.

21.72.1 Steps

1

Log in to the standalone or primary main server station as the nsp user.

2

Open a console window.

3

Copy the appropriate NE configuration archive file to the /opt/nsp/nfmp/nebackup/backup directory.

Note: An NE configuration archive file is named using the file creation time, and has the following format:
YYYY-MM-DD-hh-mm.tgz

4

Enter the following:

Note: If you intend to copy and paste the command from this step into the console window, ensure that you remove the line break from the command text before you paste the text.

```
bash$ gzip -cd /opt/nsp/nfmp/nebackup/backup/nebackup_
YYYY-MM-DD-hh-mm.tgz | tar xf - -C / ↵
```

where *YYYY-MM-DD-hh-mm*.tgz is the name of the backup file

The NE configuration files are extracted to the /opt/nsp/nfmp/nebackup directory.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

When the restore operation is complete, close the console window.

END OF STEPS

21.73 Why collect device hardware inventory data?

21.73.1 Overview

You can collect device hardware inventory data to:

- create a list of managed device objects, for example, access ports that are available as SAPs
- save for future processing and inventory tracking
- compare the current and historical lists to identify trends and capacity changes
- record the time required to gather inventory data as a base measure

See the inventory chapter in the *NSP NFM-P Classic Management User Guide* for more information about generating specific types of inventory reports.

21.74 How do I collect port inventory data for a specific managed device?

21.74.1 Process

For most inventory lists you can:

- generate an inventory of the listed data
- reorganize the information from most important to least important
- remove columns of data
- sort rows in ascending or descending order

21.74.2 Steps

1

Choose Manage→Equipment→Equipment from the NFM-P main menu. The Manage Equipment form opens.

2

Choose a Network Element (Network) and click Search. The list form displays the results of the inventory search.

3

Choose an NE from the list and click Properties. The Network Element (Edit) form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Click on the Inventory tab and choose Port (Physical Equipment). The list form displays the results of the inventory search for the selected device.

5

Generate a list based on the inventory collection or comparison that you plan to make. For example, to compare weekly lists of access ports, generate a filter to list only access ports.

6

Record the amount of time required to generate the inventory list for future base measure comparisons.

7

To show or hide columns of access port information:

1. Right-click on a column heading and choose Column Display.
2. Select Administrative State in the Displayed on Table column and click the left arrow to move the Administrative State to the Available for Table column.
3. Click Apply. The Administrative State column of data is removed from the access port list.

8

To save the list of access ports:

1. Right-click on a column heading and choose Save To File. The Save form opens.
2. Enter a filename; for example, access_device123_*dateoflistgeneration*.
3. Click Files of Type to specify the file type.
4. Browse to choose a location in which to save the file.
5. Click Save. The file is saved to the specified location with the appropriate file extension.

9

To save the table preferences for future use:

1. Right-click on a column heading and choose Save Table Preferences.
2. Click OK to confirm.

   The table preferences for the list form and user are saved. For example, when you choose another device, and click on the Ports tab and the Physical Ports tab, the Administrative State heading is not displayed. However, when you click on the SONET Channels tab, the Administrative State heading appears.

10

Move the file to another station, as required, for inventory analysis or post-processing.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.75 How do I manage main database audit logs?

21.75.1 Overview

As part of the main database security, audit log files are automatically created to track database session creation activities. The NFM-P does not automatically remove the files. You must monitor the directory that contains the audit log files to ensure that the files do not consume excessive disk space.

21.76 How do I reduce the number of Oracle audit logs?

21.76.1 Steps

1

Log in to the main database station as the Oracle management user.

Note: The Oracle management user name is specified during database installation; the default is ‘oracle’.

2

Navigate to the /opt/nsp/nfmp/oracle19/rdbms/audit directory.

3

Archive and delete the files, as required. If the number of audit files increases quickly, you may need to perform this procedure more frequently.

END OF STEPS

21.77 How do I check for performance monitoring statistics collection?

21.77.1 Process

Use the performance monitoring statistic log records to determine whether performance statistics are collected within the scheduled interval using the client GUI.

1

Choose Tools→Statistics→Statistics Manager from the NFM-P main menu. The Statistics Manager form opens.

2

Set the Statistics Type parameter to Statistics Record to retrieve a list of historical data for the type of logged statistics.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Choose a type of statistics to collect. For example, to check interface statistics for managed devices, choose Interface Additional Stats (Physical Equipment).

4

Perform one of the following:

a. To collect statistics for the past hour, click Search. Go to Step 6 .

b. To collect statistics based on a set of user-defined criteria, choose No Filter.

5

Configure the filter criteria and click Search.

Note: You must specify a filter to limit the number of log records to less than 15 000; otherwise, a problem encountered form appears.

6

Review the data for the selected statistic.

1. Click on the Monitored Object or Monitored Object Name headings to sort the historical statistics records by type of object.
2. Review the Time Captured heading for one or more objects.

   Verify that the time captured intervals match the intervals set for the object or the statistic logging class.

   If the time captured intervals are not sufficient, there will be gaps in the historical record.

7

If there are gaps in the historical record, check the mediation policy to ensure that:

- polling is enabled and administratively up
- the polling interval for a specific MIB or MIB entry is sufficient for collecting the required statistics

Note: Each row that represents a log record shows the Suspect column. When a check mark is present for an interval, there may have been a problem with collection during that interval.

8

Record the data for the selected device and type of statistics. Use this data as a base measurement to verify that statistics data was collected correctly over the scheduled interval.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Monthly maintenance

21.78 Why generate and store a user account list?

21.78.1 Overview

An NFM-P administrator must keep a record of NFM-P users in order to:

- associate staff names with user accounts
- provide account information to technical support for system access
- review user account privileges

21.79 How do I generate and store user account data?

21.79.1 Steps

1

As the admin user, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security -- Security Management (Edit) form opens.

2

Click on the Users tab.

3

Click Search without setting any filtering. The complete list of user accounts appears.

4

Organize the list of users. For example, to organize the list by the type of group that the user belongs to, click on the User Group column heading. The user accounts are listed alphabetically by user group.

5

Save the list of user accounts.

1. Right-click on the user name list heading and choose Save To File. The Save form opens.
2. Enter a name for the user account list, for example, NOCabc_useraccounts*_yearmonthday*.
3. Click on the Files of Type pull-down menu to specify the file type.
4. Browse to choose a location in which to save the file.
5. Click Save. The file is saved to the selected location in the specified format with the appropriate extension.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Move the account list to a secure location. Store the latest version of the list and keep existing versions of the list for historical purposes.

END OF STEPS

21.80 How do I test an NFM-P main database restore?

21.80.1 Purpose

It is strongly recommended that you regularly test a recent main database backup to ensure that you can use the backup to restore the database in the event of a failure.

Perform this procedure test the success of a main-database restore operation.

Note: You require root user privileges on the station that hosts the restored database.

Note: You require the Oracle management user name, group name, and password from the main database.

CAUTION

Service Disruption

Restoring a main database on a station that has connectivity to the managed network or other NFM-P components can cause a service disruption.

Ensure that you perform the procedure only on an isolated station.

Note: Before you can test a database restore on a station, you must ensure that no NFM-P software is installed on the station.

21.80.2 Steps

1

Generate comparison points for the main database, for example, the number of managed devices and cards, by creating an inventory of information, as described in the *NSP NFM-P Classic Management User Guide*. This information is used to compare against the restored database information in a test environment to check the validity of the database backup.

2

Ensure that the station on which you plan to restore the database, called the test station, has the same system configuration as the actual database station, for example, partitioning, OS version, and OS patch level.

3

Identify a recent main database backup.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

Log in to the test station as the root user.

5

Copy the database backup file set to the test station.

Note: The path to the backup file set on the test station must be the same as the path of the backup file set on the database station.

6

Transfer the following NFM-P installation files for the existing release to an empty directory on the test station:

- nsp-nfmp-jre-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-config-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-oracle-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-main-db-*R.r.p*-rel.*v*.rpm
- OracleSw_PreInstall.sh

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version identifier

7

Open a console window.

8

Navigate to the directory that contains the NFM-P installation files.

9

Enter the following:

```
# chmod +x * ↵
```

10

Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

Note: A default value is displayed in brackets []. To accept the default, press ↵.

The following prompt is displayed:

```
This script will prepare the system for a new install/restore of an
NFM-P Version R.r Rn database.
Do you want to continue? [Yes/No]:
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

12

Enter the group name of the Oracle management user from the current database deployment.

The following messages and prompt are displayed:

```
Creating group group if it does not exist ... done
Enter the Oracle user name [user]:
```

13

Enter the Oracle management user name from the current database deployment.

The following messages and prompt are displayed:

```
Oracle user [user] new home directory will be
[/opt/nsp/nfmp/oracle19].
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...
Checking user user...
Adding user...
Changing ownership of the directory /opt/nsp/nfmp/oracle19 to
user:group.
About to unlock the UNIX user [user]
Unlocking password for user user.
passwd: Success
Unlocking the UNIX user [user] completed
Please assign a password to the UNIX user user ..
New Password:
```

14

Enter the password of the Oracle management user.

The following prompt is displayed:

```
Re-enter new Password:
```

15

Re-enter the password. The following message is displayed if the password change is successful:

```
passwd: password successfully changed for user
```

The following message and prompt are displayed:

```
Specify whether an NFM-P server will be installed on this workstation.
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
The database memory requirements will be adjusted to account for the
additional load.
Will the database co-exist with an NFM-P server on this workstation
[Yes/No]:
```

16

Enter Yes or No, as required, based on the existing NFM-P deployment.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
conf...
INFO: Completed running Oracle Pre-Install Tasks
```

17

Enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

18

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

19

Enter the following:

```
# samrestoreDb path ↵
```

where *path* is the absolute path of the directory that contains the database backup file set

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The database restore begins.

If the backup file set has been created using file compression, messages like the following are displayed.

```
About to uncompress backup files under path
Completed uncompressing backup files under path
```

Messages like the following are displayed as the restore progresses.

```
Restore log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.restore.
yyyy.mm.dd-hh.mm.ss.stdout.txt
<date time> working..
<date time> Performing Step 1 of 7 - Initializing ..
<date time> Executing StartupDB.sql ...
<date time> Performing Step 2 of 7 - Extracting backup files .....
<date time> Performing Step 3 of 7 - Restoring archive log files ..
<date time> Performing Step 4 of 7 - Executing restore.rcv ..........
<date time> Performing Step 5 of 7 - Restoring Accounting tablespaces
.......
<date time> Performing Step 6 of 7 - Opening database .....
<date time> working....
<date time> Executing ConfigRestoreDB.sql ....................
<date time> working..............
<date time> Performing Step 7 of 7 - Configuring SAM Server settings
...
```

The following is displayed when the restore is complete:

```
<date time> Database restore was successful
DONE
```

20

Review the comparison points of the restored database with the actual database, as generated in Step 1 . If the databases are the same, the backup is valid and the restore operation is successful.

END OF STEPS

21.81 Why check the NFM-P platform performance?

21.81.1 Overview

Use the following procedure to test the NFM-P platform performance and to record base measures. You can compare performance monthly to:

- collect base measure information related to platform performance
- ensure that there is no degradation in performance

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If the performance degrades, collect the necessary logs and performance data and contact technical support.

21.81.2 Checking Windows client performance

You can compare Windows client station performance monthly to:

- collect base measure information related to platform performance
- ensure that there is no degradation in performance

21.82 How do I check Windows client station performance?

21.82.1 Steps

1

Open a command window on the client station.

2

Enter the following at the command prompt:

`ping station_name` ↵

where *station_name* is the IP address or hostname, if DNS is used, of the main server to which you need to test connectivity

3

Review the ping output for round-trip delays or lost packets. Resolve any connectivity issues that cause delays or dropped packets. Store ping round-trip delay or lost-packet data as a performance base measure for the station. You can use the data for future performance comparisons.

4

Open Windows Task Manager.

5

Check performance using the appropriate Task Manager tab.

a. Click on the Processes tab. A list of processes appears.

   Sort the processes by CPU usage. The name of each NFM-P process begins with javaw. The CPU usage percentage for each NFM-P process must fall within your IT specifications or the established performance base measures.

b. Click on the Performance tab. The CPU and page file usage charts appear.

   The memory and page-file usage percentages must fall within your IT specifications or the established performance base measures.

c. Click on the Networking tab. The Local Area Connection chart appears.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Network utilization greater than 10 or 20 percent may indicate collisions or other LAN problems that could affect performance in the network management domain.

6

Choose File→Exit Task Manager to close the form.

7

Open a console window.

8

Type:

`tracert station_name` ↵

where *station_name* is the IP address or hostname of the main server to which you need to test connectivity

The tracert command provides details about network connectivity.

9

Review the tracert data, including:

- number of hops required to reach the main server
- average time between hops

Record the data for future base measure comparison. For example, when the number of hops between a client GUI and main server increases over time, traffic takes longer to travel between them, which can degrade performance.

10

Check regularly for advisories related to the OS. If updates or patches are required, contact technical support for information about potential effects on the NFM-P.

END OF STEPS

21.83 How do I check network connections between components?

21.83.1 Overview

Use the ping and traceroute functions each month to check LAN TCP/IP connectivity between NFM-P components, and track the measurements over time to establish trends for extrapolation during network planning, and to identify changes in latency. Contact your IT department if you suspect a communication problem between components.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

21.84 How do I measure NFM-P performance?

21.84.1 Steps

1

Log into a main server, auxiliary server, or main database station as the root user.

2

Open a console window.

3

Enter the following to list the processes that have the highest CPU usage:

```
# top ↵
```

Depending on your system configuration, approximately the top 20 processes are displayed. The top NFM-P process, by CPU usage, is typically the Java process.

4

Review the output; see the top man page for a description of the output fields.

5

Record the data for future performance comparison. Look for data that indicates excessive or continuously increasing CPU usage by the Java process.

6

Press Ctrl+C to stop the command.

7

Enter the following to list CPU resource usage information:

```
# mpstat nn ↵
```

where *nn* is the time, in seconds, between CPU polls; a value between 10 and 60 is recommended

8

Review the command output; see the mpstat man page for a description of the output fields.

9

Record the data for future performance comparison. Look for a difference in the output for a similar load on each station; a difference may indicate CPU performance degradation.

10

Press Ctrl+C to stop the command.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Enter the following to list disk performance information:

iostat -x *n* ↵

where *nn* is the time, in seconds, during which you want to collect data; a starting value of 2 is recommended

12

Review the output; see the iostat man page for a description of the output fields.

13

Record the data for future performance comparison. Look for a difference in the output for a similar load on each station that may indicate disk performance degradation on a station.

14

Press Ctrl+C to stop the command.

15

Use an OS command to list network interface throughput and error statistics.

16

Record the data for future performance comparison. Look for a difference in the output for a similar load on each station that may indicate network performance degradation.

17

Close the console window.

END OF STEPS

21.85 How do I check network management connections?

21.85.1 Steps

1

Open a console window on the station.

2

Ping the hostname of another station in the network management domain by entering the following:

ping *station_name* ↵

where *station_name* is the IP address or hostname of the other station

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3

Review the output. The following is an example of ping output:

```
PING station_name: 56 data bytes
64 bytes from hostname (IP_address): icmp_seq=0, time=nnn ms
64 bytes from hostname (IP_address): icmp_seq=1, time=nnn ms
64 bytes from hostname (IP_address): icmp_seq=2, time=nnn ms
----station_name PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/1
```

LAN congestion may be a problem if packets are received out of order, are dropped, or take too long to complete the round trip.

4

Store the output for future base measure comparison.

Compare the output over time to ensure that changes in the data are not caused by deteriorating LAN conditions.

5

Check the routing information.

1. Open a console window on the station.
2. Enter one of the following traceroute commands to determine the path taken to a destination by an ICMP echo request message:
   - traceroute ↵ on a RHEL station
   - tracert ↵ on a Windows station

   The list of near-side interfaces in the path between a source host and a destination device is displayed. The near-side interfaces are the interfaces closest to the source host.

6

Store the output as a record for future base measure comparisons. Compare routes over time to ensure that there is optimal connectivity.

7

To check the routing tables for the platform:

1. Open a console window on the station.
2. To view the active routes for the platform, type:

   netstat -rn ↵

   The following information is displayed:
   - network destination and gateway IP addresses
   - gateway used to reach the network destination
   - IP address of the interface on which communication occurs
   - metric value of the route

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Store the output as a record for future base measure comparison. Compare routes over time to ensure that there is optimal connectivity.

END OF STEPS

21.86 How do I test main server and database redundancy switches?

21.86.1 Overview

In a redundant NFM-P system, performing regular main server and database redundancy tests is important for the following reasons:

- to ensure that main server and database redundancy functions correctly and responsively
- to identify conditions that may interfere with an NFM-P upgrade

Note: It is strongly recommended that you perform a main server activity switch and a database switchover monthly, or at least quarterly, if a monthly test is not possible. For information about performing a server activity switch, see 16.11 “How do I perform a server activity switch?” (p. 484) . For database switchover information, see 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) or 16.14 “How do I perform a main database switchover using a CLI script?” (p. 487). Contact technical support for further assistance.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22 Classic management database administration

22.1 What is the NFM-P main database?

22.1.1 Description

This section describes the NFM-P main database, and how to manage the associated data integrity and security functions.

An NFM-P main database stores classic mediation network data that includes object configurations, device backups, and statistics: The NFM-P uses the data to create a network model for use by NFM-P management functions.

An NFM-P system requires a central, Oracle-based database for persistent storage. The database can be on the same station as the main server, or on a separate station. A redundant NFM-P deployment has two identical main database instances in a synchronized primary/standby configuration to limit data loss in the event of a failure.

You can manage the following database functions and parameters:

- security
- statistics data retention
- data synchronization
- backups and restores
- historical record retention
- object ageout
- log storage
- error monitoring
- alarm handling

See “NFM-P Oracle database” in the *NSP Planning Guide* for more information about licensing and support for the Oracle 19c Enterprise Edition embedded with the NFM-P main database installation.

22.1.2 Backups and restores

It is strongly recommended that you schedule regular NFM-P main database backups through the NFM-P client UI. You can also initiate a backup operation manually on demand either through the UI or via CLI.

An NFM-P main database backup operation is performed on the standalone or active main database station. In a redundant NFM-P system, the NFM-P automatically copies the database backup files to the standby database station if database backup file synchronization is enabled. The following information is saved in the backup operation:

- device inventory
- infrastructure configurations
- service configurations
- STM configurations
- alarms
- performance statistics (if configured for database storage and if retention policy set appropriately)

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- accounting statistics (if configured for database storage and if retention policy set appropriately); note that accounting statistics are excluded if you select partial backup
- file-based statistics (if configured for database storage; file-based statistics configured as “file only” are not included)
- user and role data
- system settings configured from the NFM-P client UI

The following information is **not** stored in the NFM-P main database and is therefore **not** saved during the backup operation:

- server or database custom configurations, such as customizations made in the nms-server.xml file
- installation binaries and images
- license records
- raw log archives
- external directory data
- NE configuration backup files, which are saved to the main server file system; see 21.69 “How do I back up and restore NE configuration files?” (p. 687)
- **non**-NFM-P data such as workflows, analytics, real-time telemetry counters, reference tables, and audit logs

An NFM-P main database backup can be restored as described in 22.2 “How do I restore and reinstantiate the NFM-P main database?” (p. 709)

22.1.3 Main database safeguards

In addition to the protection of system redundancy, the NFM-P has mechanisms that raise alarms for the following:

- database disk and tablespace capacity issues
- redundancy events, misconfiguration, and failures
- database backup misconfiguration and failures
- archive log management actions and failures
- internal errors that may represent a security risk
- size constraint and ageout constraint policy violations

22.1.4 References

See the following for more information:

- *NSP Planning Guide*—main database platform and network requirements
- *NSP Installation and Upgrade Guide*—main database deployment
- *NSP Troubleshooting Guide*—main database troubleshooting
- NSP NFM-P Alarm Search Tool—alarm descriptions, raising and clearing conditions, and remedial actions

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.2 How do I restore and reinstantiate the NFM-P main database?

22.2.1 Description

CAUTION

Service Disruption

A main database restore requires a shutdown of each main database and main server in the NFM-P system, which causes a network management outage.

You must perform a database restore only during a scheduled maintenance period, and contact technical support before you attempt to restore a main database.

You can restore a main database using a backup copy.

In a redundant system, you must perform one or both of the following to regain main database function and redundancy, depending on the failure type.

- Restore the primary main database.
- Reinstantiate the standby main database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinstantiate the primary database on the standby database station to restore redundancy. You can use the NFM-P client GUI or a CLI script to reinstantiate a database.

Note: In a redundant system, you can restore a main database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the main database, if it is installed.
- Install a primary database on the station.

In a redundant system, you can reinstantiate a database only on a standby database station. To reinstantiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinstantiation:

- Uninstall the main database, if it is installed.
- Install a standby database on the station.

Note: A main database restore requires that the Oracle home version matches the Oracle version of the database backup. If you do not reinstall the Oracle software, for example, when you restore on the same station, the restore procedure is unchanged. If you reinstall the Oracle software, for example, when you restore on a new station, and the database backup was created while an NFM-P service pack that upgrades the Oracle software was applied, you must raise the Oracle version to the backup level before you restore the database; see 22.16 “How do I restore the primary main database in a redundant system?” (p. 735) .

See 22.15 “How do I restore a standalone main database?” (p. 727) for information about restoring a standalone main database. See 22.16 “How do I restore the primary main database in a redundant system?” (p. 735) for information about restoring a redundant main database. See 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) and 22.21 “How do I

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

reinstantiate the main database from a CLI?” (p. 715) for information about reinstantiating a primary main database on a standby database station.

22.3 Pathway: NFM-P database management

22.3.1 Stages

Note: It is strongly recommended that you verify the checksum of each file that you download from the NSP download page on the Nokia Support portal. You can compare the SHA-256 checksum value in the Packages.sha256sum on the download page to the output of the RHEL sha256sum command. See the RHEL sha256sum man page for information.

Database properties and status

1

Display the main database properties; see 22.4 “How do I view the main database properties?” (p. 712) .

Database operation and security

2

As a security precaution, configure the number of failed Oracle database user login attempts that the NFM-P allows before a user is locked out; see 22.5 “How do I configure the Oracle database user lockout threshold?” (p. 713) .

3

As required, unlock the Oracle database user account after multiple login failures; see 22.6 “How do I unlock the Oracle database user account?” (p. 715) .

4

Configure how the NFM-P responds to Oracle database errors; see 22.7 “How do I configure Oracle database error monitoring?” (p. 716) .

5

Configure size constraint policies to regulate the number of records retained in the main database; see 22.8 “How do I configure a size constraint policy?” (p. 716) .

6

Configure ageout constraint policies to define a configurable ageout time for a specific object type in the main database; see 22.9 “How do I configure an ageout constraint policy?” (p. 718) .

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

7

Manage main database disk usage by configuring policies to manage the file size and number of archive log and core dump files; see 22.10 “How do I create a database file policy to manage database log or core dump files?” (p. 719) .

8

Configure the statistics data retention period for the main database; see 22.11 “How do I configure the statistics data retention period for the main database?” (p. 721) .

Backup, restore, and maintenance

9

Perform an immediate full or partial main database backup; see 22.12 “How do I back up the main database from the client GUI?” (p. 721) or 22.13 “How do I back up the main database from a CLI?” (p. 723) .

10

Schedule a regular main database backup; see 22.14 “How do I schedule main database backups?” (p. 726) .

11

Restore the main database in a standalone system; see 22.15 “How do I restore a standalone main database?” (p. 727).

12

Restore the main database in a redundant system; see 22.16 “How do I restore the primary main database in a redundant system?” (p. 735).

13

As required, delete the inactive residential subscriber instances from the main database; see 22.17 “How do I delete the inactive residential subscriber instances?” (p. 746).

14

Test the main database restore function to ensure that main database backups are viable in the event of a failure; see 21.80 “How do I test an NFM-P main database restore?” (p. 696) .

15

Export a main database to a file set; see 22.18 “How do I export an NFM-P main database?” (p. 748).

16

Import a main database from a file set; see 22.19 “How do I import an NFM-P main database?” (p. 752).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

17

Verify the synchronization of NE and main database information; see 21.67 “How do I check the main database performance?” (p. 684) .

Redundancy functions

18

Perform a main database switchover; see 16.12 “How do I configure main database switchover behavior?” (p. 485) , 16.13 “How do I perform a main database switchover using the NFM-P client GUI?” (p. 486) , or 16.14 “How do I perform a main database switchover using a CLI script?” (p. 487) .

19

Enable or disable automatic database realignment on a main server; see 16.15 “How do I enable or disable automatic database realignment?” (p. 488).

20

Re-establish redundancy after a database activity switch or similar maintenance activity; see 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) and 22.21 “How do I reinstantiate the main database from a CLI?” (p. 756).

22.4 How do I view the main database properties?

22.4.1 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager (Edit) form opens and displays information that includes the following:

- Database Name
- Instance Name
- Listener Port—the port on the main server for database communication
- DBID—the Oracle database ID, sometimes called the SID
- Creation Time—the database creation time
- Version—the Oracle version identifier
- IP Address—the database IP address that the main and auxiliary servers use
- Host Name—the database station hostname
- Open Mode—specifies the type of database access
- Archive Log Mode—specifies whether to archive the database log files; configured during database installation
- Protection Mode—the database protection mode, which cannot be changed

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2

View the information.

3

Close the Database Manager (Edit) form.

END OF STEPS

22.5 How do I configure the Oracle database user lockout threshold?

22.5.1 Purpose

As a security precaution, you can configure the number of consecutive Oracle database user login failures that are tolerated before the user account is locked.

If the Oracle database user account is locked because of too many login failures, you can unlock the account by performing 22.6 “How do I unlock the Oracle database user account?” (p. 715).

Note: In a redundant deployment, you perform the procedure on the primary database station. After you perform the procedure, the primary database automatically copies the configuration change to the standby database.

The configuration change that you make in this procedure is not affected by a subsequent database upgrade.

22.5.2 Steps

1

Log in to the main database station as the Oracle management user or the NSP admin user.

Note: The Oracle management user name is specified during database installation; the default is ‘oracle’.

2

Open a console window.

3

Enter the following:

Note: If you are logged in as the NSP admin user, you must use sudo to run the command in this step as shown in the following:
sudo -u oracle *path/command*

```
bash$ /opt/nsp/nfmp/db/install/config/samdb/SAMDb_security.sh ↵
```

The following prompt is displayed:

```
Please select one of the following options:
  1) Setting failed login attempts
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
 2) Unlock database user
0) Exit
Please enter(1,2 or 0):
```

4

Enter 1 ↵.

The following prompt is displayed:

```
Please select one of the following options:
   1) Setting the number of failed login attempts
   2) Remove the number of failed login attempts setting (no checking)
   0) Exit
   Please enter(1,2 or 0):
```

5

To specify the allowed number of login failures, perform the following steps.

1. Enter 1 ↵.

   The following prompt is displayed:

   ```
   This value will be used for setting the number of failed login
   attempts before locking the database user account.
   Please enter value for number of failed login attempts(20 to 1000)
   (30):
   ```

2. Specify a value between 20 and 1000 and press ↵.

   The following messages are displayed:

   ```
   About to change the Oracle database user settings
   Completed changing the Oracle database user settings
   ```

3. Go to Step 7 .

6

To disable checking for failed login attempts, enter 2 ↵.

The following messages are displayed, and the NFM-P no longer locks the Oracle database user account after multiple login failures.

```
About to change the Oracle database user settings
Completed changing the Oracle database user settings
```

7

Close the console window.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.6 How do I unlock the Oracle database user account?

22.6.1 Purpose

Perform this procedure to unlock the locked Oracle database user account.

22.5 “How do I configure the Oracle database user lockout threshold?” (p. 713) describes how to configure the account lockout criteria.

Note: In a redundant deployment, you perform the procedure on the primary database station. After you perform the procedure, the primary database automatically copies the configuration change to the standby database.

The configuration change that you make in this procedure is not affected by a subsequent database upgrade.

22.6.2 Steps

1

Log in to the main database station as the Oracle management user or the NSP admin user.

Note: The Oracle management user name is specified during database installation; the default is ‘oracle’.

2

Open a console window.

3

Enter the following:

Note: If you are logged in as the NSP admin user, you must use sudo to run the command in this step as shown in the following:
`sudo -u oracle path/command`

```
bash$ /opt/nsp/nfmp/db/install/config/samdb/SAMDb_security.sh ↵
```

The following prompt is displayed:

```
Enter the password for the "sys" user (terminal echo is off):
```

4

Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
Please select one of the following options:
  1) Setting failed login attempts
  2) Unlock database user
  0) Exit
 Please enter(1,2 or 0):
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Enter 2 ↵.

The following messages are displayed, and the Oracle database user account is unlocked.

```
About to unlock the database user username
Completed unlocking the database user username
```

6

Close the console window.

END OF STEPS

22.7 How do I configure Oracle database error monitoring?

22.7.1 Purpose

You can configure how the NFM-P handles Oracle database errors to provide monitoring information that may help with troubleshooting or the detection of security violations such as SQL injection attacks. When database error monitoring is enabled, the NFM-P raises an alarm when the Oracle software reports an error, for example, an invalid SQL statement.

22.7.2 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager (Edit) form opens.

2

To enable database error monitoring, select the Enable Database Error Monitoring parameter.

3

To disable database error monitoring, deselect the Enable Database Error Monitoring parameter.

4

Save your changes and close the form.

END OF STEPS

22.8 How do I configure a size constraint policy?

22.8.1 Purpose

Size constraint policies regulate the number of historical records that the main database retains before purging records. The scheduling of tasks through the NFM-P can generate a large volume of

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

archived result information if left unchecked. Size constraint policies control the volume of information stored by defining thresholds for various record classes. When the number of records for a specific class or group of classes reaches a threshold specified in the policy, the NFM-P deletes a specified number of the oldest objects that are associated with the class or group of classes.

22.8.2 Steps

1

Choose Administration→Constraint Policies→Size Constraint Policies from the NFM-P main menu. The Size Constraint Policies form opens.

2

Click Create or choose a policy and click Properties. The Size Constraint Policy (Create | Edit) form opens.

Note: The NFM-P is preconfigured with the following default size constraint policies for various record classes:

- Script Management Results
- Clear Requests
- CPAM Protocol Data
- Work Order Import Logs
- LTE User Stats Query Output Snapshots

3

Configure the general policy parameters.

4

Click on the Constrained Packages tab.

5

Right-click on the Size Constraint Policy icon and choose Select Packages.

6

Choose a size constraint package and click OK. The package appears in the navigation tree under the Size Constraint policy. Go to Step 7 if the package selected supports a sub-class package, for example, the dhcp package supports three sub-class packages. Otherwise, go to Step 9 .

7

Right-click on the package icon and choose Select Classes. The Select Size Constrained Classes form opens.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

Choose a sub-class package and click OK to Save your changes and close the form.

9

Close the Size Constraint Policy (Create|Edit) form.

END OF STEPS

22.9 How do I configure an ageout constraint policy?

22.9.1 Purpose

An ageout constraint policy defines the database ageout period for a specific object type. When the age of an object reaches the ageout value, the NFM-P deletes the object from the database.

The NFM-P supports ageout constraint policies to define the period of time the database retains persisted virtual network objects. These policies are the dctr policies listed below.

Note: The NFM-P has a number of preconfigured ageout constraint policies.

22.9.2 Steps

1

Choose Administration→Constraint Policies→Ageout Constraint Policies from the NFM-P main menu. The Ageout Constraint Policies form opens.

2

Select a policy and click Properties. The Ageout Constraint Policy form opens.

3

Review the Object Count information in the Status panel. The information refers to the most recent object deletion, and can help you define the appropriate ageout time and deletion interval values for the policy.

4

Configure the parameters.

Note: The Qualified Ageout Time defaults are guidelines. Consider the following when setting the Qualified Ageout Time:

- A small value can prevent excessive database table growth.
- The value must be great enough to allow sufficient time to upload the database records to a third-party utility.

5

Save your changes and close the form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

CAUTION

Service Disruption

Modifying the server configuration can have serious consequences including service disruption.

Contact technical support before you attempt to modify the server configuration.

If required, edit the ageout constraint policy configuration file to modify the following parameters in the Deletion Interval panel:

- Synchronization Time—shown as ageoutSyncTime in the configuration file
- Interval (hours)—shown as ageoutInterval in the configuration file

Note: You must perform the following steps on each main server in the NFM-P system.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Navigate to the /opt/nsp/nfmp/server/nms/config directory.
4. Open the AgeoutConstraints.xml file using a plain-text editor.
5. Locate the following XML tag:

   ```
   <ageout>
   ```

6. Locate the object class section that you need to modify; the following code shows the residential subscriber instance object class as an example:

   ```
   <class name="ressubscr.ResidentialSubscriberInstance"
     ageoutSyncTime="00:00"
     ageoutInterval="1">
   /class>
   ```

7. Modify the ageoutSyncTime and ageoutInterval values, as required.
8. Save and close the AgeoutConstraints.xml file.
9. On a standalone main server, or the primary main server in a redundant system, enter the following:

   ```
   bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read_config ↵
   ```

   The NFM-P puts the configuration change into effect.
10. Close the console window.

END OF STEPS

22.10 How do I create a database file policy to manage database log or core dump files?

22.10.1 Purpose

You can create database file policies to manage the file size and number of archives for stored

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

alert, listener, trace, audit, and core dump files. When the size and number of files are left unbounded, excessive database disk capacity is consumed.

Database trace, alert, and audit log files are compressed and stored in the alert log directory. Database listener log files are stored in the listener log directory.

Note: For historical or troubleshooting purposes, recommends that you archive the main database log files on a regular basis.

22.10.2 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager (Edit) form opens.

2

Click on the File Policies tab.

3

Click Database File Policies or choose a default policy and click Properties. The Database File Policies Create | Edit) form opens. If you selected a default policy, go to Step 5 .

4

Click Create.

5

Configure the required general file policy parameters and Purge Details panel parameters.

6

Click OK to save your changes and close the form.

7

If required, click Select to apply the new purge details to a default policy.

8

Save your changes and close the Database Manager (Edit) form.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.11 How do I configure the statistics data retention period for the main database?

22.11.1 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager (Edit) form opens.

2

CAUTION

Service Disruption

Configuring the parameter can seriously affect NFM-P system performance.

Consult technical support before you configure the parameter.

Configure the Accounting Statistic Data Retention Period (Days) parameter.

3

Save your changes and close the Database Manager (Edit) form.

END OF STEPS

22.12 How do I back up the main database from the client GUI?

22.12.1 Purpose

Perform this procedure to initiate an on-demand main database backup using the client GUI. You can perform a full backup, which includes the contents of the database as described in 22.1.2 “Backups and restores” (p. 707), or a partial backup, which excludes accounting statistics data.

CAUTION

Service Disruption

The disk partition that is to contain the database backup must have sufficient space for the database backup file set.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the NSP Planning Guide.

Note: The NFM-P backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the NFM-P automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstantiation.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: During a database backup, the performance of GUI or XML API operations may be affected. It is recommended that you perform a database backup only during a period of low NFM-P activity.

22.12.2 Steps

1

Choose Administration→Database from the NFM-P main menu. The Database Manager form opens.

2

Click on the Backup tab.

3

CAUTION

Data Loss

Before the NFM-P performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify does not contain files that you need to retain.

CAUTION

Data Loss

The Manual Backup Directory path must not include the main database installation directory, or data loss may occur.

Ensure that the directory path does not include /opt/nsp/nfmp/db.

Note: The Oracle management user requires read and write permissions on the backup directory. The user and group names are specified during database installation; the default is ‘oracle’ in the ‘dba’ group.

Configure the following parameters:

- Manual Backup Directory
- Enable Backup File Compression

4

Perform one of the following.

a. Click Partial Backup.

b. Click Full Backup.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Click Yes. The full or partial backup operation begins, and the Backup State indicator reads In Progress.

Depending on the database size, a backup may take considerable time.

6

If required, monitor the Backup Status information, which includes the following:

- Scheduled Backup—whether scheduled backup is configured
- Backup State—state of current backup operation; dynamically updated
- Next Scheduled Backup Time—time of next scheduled backup
- Last Successful Backup Time—completion time of latest successful backup
- Last Successful Backup Type—type of latest successful backup
- Last Attempted Backup Time—when latest attempted backup began
- Last Attempted Backup Type—type of latest attempted backup
- Directory of the Last Successful Backup—location of latest successful backup
- Host Name of the Last Successful Backup—hostname of station that performed latest successful backup

7

Close the Database Manager (Edit) form.

The database backup creates the following summary file in the same directory as the backup files:

BACKUP_SUMMARY.INFO

The summary file contains detailed backup information that includes the backup completion time, and the name and size of each backup file.

END OF STEPS

22.13 How do I back up the main database from a CLI?

22.13.1 Purpose

Perform this procedure to initiate an on-demand main database backup using CLI. You can perform only a full database backup from a CLI. To perform a partial backup, see 22.12 “How do I back up the main database from the client GUI?” (p. 721).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

CAUTION

Service Disruption

The disk partition that is to contain the database backup must have sufficient space for the database backup file set, or system performance may be compromised.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the NSP Planning Guide.

Note: The NFM-P backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the NFM-P automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstantiation.

Note: During a database backup, the performance of GUI or XML API operations may be affected. It is recommended that you perform a database backup only during a period of low NFM-P activity.

22.13.2 Steps

1

Log in as the root user on the main database station.

Note: In a redundant NFM-P system, you must log in to the primary database station.

2

Open a console window.

3

CAUTION

Data Loss

Before the NFM-P performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify in this step does not contain files that you need to retain.

CAUTION

Data Loss

The backup directory path must not include the main database installation directory, or data loss may occur.

Ensure that the directory path does not include /opt/nsp/nfmp/db.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The Oracle management user requires read and write permissions on the backup directory. The user and group names are specified during database installation; the default is ‘oracle’ in the ‘dba’ group.

Perform one of the following.

a. Enter the following to back up the database without using file compression:

```
# sambackupDb backup_directory ↵
```

where *backup_directory* is the absolute path of the directory that is to contain the database backup file set

b. Enter the following to back up the database using file compression:

```
# sambackupDb backup_directory compress ↵
```

where *backup_directory* is the absolute path of the directory that is to contain the database backup file set

Note: Depending on the database size, a backup may take considerable time.

The database backup begins, and messages like the following are displayed as the backup progresses:

```
Backup log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.backup.
yyyy.mm.dd-hh.mm.ss.stdout.txt
<date time> working..
<date time> Performing Step 1 of 4 - Initializing ..
<date time> Performing Step 2 of 4 - Backup archive logs ..
<date time> Performing Step 3 of 4 - Backup the database ..........
<date time> Performing Step 4 of 4 - Finalizing  .....
```

The following is displayed when the backup is complete:

```
<date time> Database backup was successful
DONE
```

4

When the backup is complete, close the console window.

The database backup creates the following summary file in the same directory as the backup files:

BACKUP_SUMMARY.INFO

The summary file contains detailed backup information that includes the backup completion time, and the name and size of each backup file.

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.14 How do I schedule main database backups?



CAUTION

Service Disruption

The disk partition that is to contain the database backup must have sufficient space for the database backup file set, or system performance may be compromised.

Ensure that the backup directory is at least five times as large as the expected database backup size. For more information, contact technical support or see the NSP Planning Guide.



CAUTION

Service Disruption

A main database backup consumes considerable system resources.

Ensure that you specify a backup schedule of reasonable frequency, for example, daily.

Note: The NFM-P backs up the Oracle encryption wallet during a database backup, and restores the wallet during a database restore. In a redundant deployment, the NFM-P automatically replicates the encryption wallet from the primary to the standby database after the standby database reinstantiation.

Note: During a database backup, the performance of GUI or XML API operations may be affected. It is recommended that you schedule the database backup to occur during a period of low NFM-P activity.

22.14.1 Steps

1

Choose Administration→Database from the NFM-P menu. The Database Manager form (Edit) opens.

2

Click on the Backup tab.

3

Configure the required parameters in the Backup Schedule panel.

Note: You must select the Schedule Enabled parameter.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

4

CAUTION

Data Loss

Before the NFM-P performs a database backup, it deletes the contents of the specified backup directory.

Ensure that the backup directory that you specify in this step does not contain files that you need to retain.

Configure the Scheduled Backup Directory parameter in the Backup Setting panel. The value that you specify is the database station directory in which to save the backup file sets. Each file set is stored in a subdirectory named backupset*n*, where *n* is a sequential number; the highest possible value is the Number to Keep parameter value.

Note: The Oracle management user requires read and write permissions on the backup directory. The user and group names are specified during database installation; the default is 'oracle' in the 'dba' group.

Note: The Scheduled Backup Directory must be a directory on the local file system.

5

Close the Database Manager form.

6

After each scheduled database backup completes, move the database backup file set to another station for safekeeping.

The database backup creates the following summary file in the same directory as the backup files:

BACKUP_SUMMARY.INFO

The summary file contains detailed backup information that includes the backup completion time, and the name and size of each backup file.

END OF STEPS

22.15 How do I restore a standalone main database?

22.15.1 Purpose

The following steps describe how to restore a standalone main database using a backup file set. You require the following:

- a database backup file set from the same NFM-P release
- the original file path of the database backup

Note: You require the following user privileges:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

- main server — root, nsp
- main database — root, Oracle management user

Note: The Oracle management user requires read and write permissions on the backup directory. The user and group names are specified during database installation; the default is ‘oracle’ in the ‘dba’ group.

22.15.2 Steps

1

If the database backup file set is on the database station, copy the file set to a different station for safekeeping.

2

Perform the following steps to stop the main server.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```
4. Enter the following to stop the main server:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```
5. Enter the following to display the NFM-P server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

3

Enter the following to switch to the root user:

```
bash$ su ↲
```

4

Enter the following to disable the automatic main server startup.

```
# systemctl disable nfmp-main.service ↲
```

5

If you are restoring the database on a new station, for example, if the current database station is unusable, go to Step 10.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

6

Log in to the database station as the root user.

7

Enter the following to uninstall the database:

```
# dnf remove nsp-nfmp-main-db --setopt=clean_requirements_on_remove=
false ↵
```

The dnf utility displays the following prompt:

```
Installed size: nn G
Is this ok [y/N]:
```

8

Enter y. The following is displayed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Uninstalling the NFM-P Database...
```

When the uninstallation is complete, the following is displayed:

```
Complete!
```

9

When the uninstallation is complete, enter the following to reboot the database station:

```
# systemctl reboot ↵
```

The station reboots.

10

Log in as the root user on the database station.

11

Open a console window.

12

Remove any files in the /opt/nsp/nfmp/db/tablespace and /opt/nsp/nfmp/db/archivelog directories.

13

Copy the database backup file set to the station.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The path to the backup file set must be the same as the path to the file set at creation time.

14

Perform one of the following.

a. If you are restoring the database on the same station, download or copy the following NFM-P installation files for the existing release to an empty directory on the database station:
   - nsp-nfmp-main-db-*R.r.p*-rel.*v*.rpm
   - OracleSw_PreInstall.sh

b. If you are restoring the database on a new station, for example, if the current database station is unusable, download or copy the following NFM-P installation files for the existing release to an empty directory on the database station:

- nsp-nfmp-jre-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-config-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-oracle-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-main-db-*R.r.p*-rel.*v*.rpm
- OracleSw_PreInstall.sh

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version identifier

15

Navigate to the directory that contains the NFM-P installation files.

Note: Ensure that the directory contains only the installation files.

16

Enter the following:

```
# chmod +x * ↵
```

17

Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

Note: The default values displayed by the script are shown as [*default*]. To accept a default value, press ↵.
The following prompt is displayed:

```
This script will prepare the system for a new install/restore of
an NFM-P Version R.r Rn database.
Do you want to continue? [Yes/No]:
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

18

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

19

Enter a group name and press ↵.

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following message is displayed:

```
Creating group group if it does not exist...
```

If you specify a new group, the following message is displayed:

```
done
```

20

If you specify an existing group, the following prompt is displayed:

```
WARNING: Group group already exists locally.
Do you want to use the existing group? [Yes/No]:
```

Perform one of the following.

a. Enter Yes ↵.

b. Enter No ↵. Go to Step 19 .

21

If the default user exists in the specified group, the following prompt is displayed:

```
The user [username] for the group [group] already exists locally.
Do you want to use the existing user? [Yes/No]:
```

22

Perform one of the following.

a. Enter Yes ↵; the following messages are displayed:

```
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...
Checking user username...
WARNING: Oracle user with the specified name already exists locally.
Redefining the primary group and home directory of user username ...
usermod: no changes
Changing ownership of the directory /opt/nsp/nfmp/oracle19 to
username:group.
About to unlock the UNIX user [username]
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Unlocking password for user username
passwd: Success Unlocking the UNIX user [username] completed
```

b. Enter No ↵. The following prompt is displayed:

```
Enter the Oracle user name:
```

Type a username and press ↵.

The following messages and prompt are displayed:

```
Oracle user [username] new home directory will be
[/opt/nsp/nfmp/oracle19].
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19..
Checking user username...
Adding username...
Changing ownership of the directory /opt/nsp/nfmp/oracle19 to
username:group.
About to unlock the UNIX user [username]
Unlocking password for user username.
passwd: Success
Unlocking the UNIX user [username] completed
Please assign a password to the UNIX user username ..
New Password:
```

23

Perform one of the following.

a. If you specify a new user in Step 22 , the following prompt is displayed:

```
Please assign a password to the UNIX user username ..
New Password:
```

Perform the following steps.

1. Type a password and press ↵. The following prompt is displayed:

   ```
   Re-enter new Password:
   ```

2. Retype the password and press ↵. The following message is displayed if the password update is successful:

   ```
   passwd: password successfully changed for username
   ```

b. If you specify an existing user in Step 22 , the following prompt is displayed:

```
Do you want to change the password for the UNIX user username?
[Yes/No]:
```

Type No ↵.

24

The following prompt is displayed:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Specify whether an NFM-P server will be installed on this workstation.
The database memory requirements will be adjusted to account for the
additional load.
Will the database co-exist with an NFM-P server on this workstation
[Yes/No]:
```

Enter Yes or No, as required, and press ↵.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
conf...
INFO: Completed running Oracle Pre-Install Tasks
```

25

When the script execution is complete, enter the following to reboot the database station:

```
# systemctl reboot ↵
```

The station reboots.

26

When the reboot is complete, log in as the root user on the database station.

27

Navigate to the directory that contains the NFM-P installation files.

28

Perform one of the following:

a. If you are restoring the database on the same station, enter the following:

```
# dnf install nsp-nfmp-main-db* ↵
```

b. If you are restoring the database on a new station, enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

29

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

30

Enter the following:

samrestoreDb *path* ↵

where *path* is the absolute path of the directory that contains the database backup file set

The database restore begins.

If the backup file set has been created using file compression, messages like the following are displayed.

```
About to uncompress backup files under path
Completed uncompressing backup files under path
```

Messages like the following are displayed as the restore progresses.

```
Restore log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.restore.
yyyy.mm.dd-hh.mm.ss.stdout.txt
<date time> working..
<date time> Performing Step 1 of 7 - Initializing ..
<date time> Executing StartupDB.sql ...
<date time> Performing Step 2 of 7 - Extracting backup files .....
<date time> Performing Step 3 of 7 - Restoring archive log files ..
<date time> Performing Step 4 of 7 - Executing restore.rcv ..........
<date time> Performing Step 5 of 7 - Restoring Accounting tablespaces
.......
<date time> Performing Step 6 of 7 - Opening database .....
<date time> working....
<date time> Executing ConfigRestoreDB.sql ...................
<date time> working..............
<date time> Performing Step 7 of 7 - Configuring SAM Server settings
...
```

The restore is complete when the following is displayed:

```
<date time> Database restore was successful
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
DONE
```

31

Log in to the main server station as the root user.

32

Enter the following to enable the automatic main server startup.

```
# systemctl enable nfmp-main.service ↵
```

33

Start the main server.

1. Enter the following to switch to the nsp user:

   ```
   # su - nsp ↵
   ```

2. Enter the following:

   ```
   bash$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash start ↵
   ```

   The main server starts.

34

Close the open console windows, as required.

35

Perform a full network resynchronization to discover the interim changes in the managed network.

END OF STEPS

22.16 How do I restore the primary main database in a redundant system?

22.16.1 Purpose

The following steps describe how to restore the primary main database in a redundant NFM-P system using a backup file set created on the same station. The station is called the primary database station in the procedure.

To regain main database redundancy after a database restore, you must reinstantiate the primary database on the standby database station. See 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) and 22.21 “How do I reinstantiate the main database from a CLI?” (p. 756) for information.

You require the following:

- a main database backup file set from the same NFM-P release
- the original file path of the database backup

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: If you reinstall the Oracle software, for example, when you restore the database on a new station, the Oracle home version must match the Oracle version of the database backup. If the backup was created while an NFM-P service pack that upgrades the Oracle software was applied, you must apply the matching service pack before you restore the database, as described in this procedure.

Note: You require the following user privileges:

- main server — root, nsp
- main database — root, Oracle management user

Note: The Oracle management user requires read and write permissions on the backup directory. The user and group names are specified during database installation; the default is ‘oracle’ in the ‘dba’ group.

22.16.2 Steps

1

If the database backup file set is on the primary database station, copy the file set to a different station for safekeeping.

2

Stop the standby main server.

1. Log in to the standby main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```
4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```
5. Enter the following to display the server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

3

Enter the following to switch to the root user:

```
bash$ su ↵
```

4

Enter the following to disable the automatic main server startup.

```
# systemctl disable nfmp-main.service ↵
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Stop the standby database:

1. Log in to the standby database station as the root user.
2. Open a console window.
3. Enter the following to stop the Oracle proxy:

   ```
   # systemctl stop nfmp-oracle-proxy.service ↵
   ```

4. Enter the following to stop the database:

   ```
   # systemctl stop nfmp-main-db.service ↵
   ```

6

Stop the primary main server.

1. Log in to the primary main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following to display the server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

7

Enter the following to switch to the root user:

```
bash$ su ↵
```

8

Enter the following to disable the automatic main server startup.

```
# systemctl disable nfmp-main.service ↵
```

9

If you are restoring the database on a new station, for example, if the current primary database station is unusable, go to Step 15.

10

Log in to the primary database station as the root user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Open a console window.

12

Enter the following to uninstall the primary database:

```
# dnf remove nsp-nfmp-main-db --setopt=clean_requirements_on_remove=
false ↵
```

The dnf utility displays the following prompt:

```
Installed size: nn G
Is this ok [y/N]:
```

13

Enter y. The following is displayed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Uninstalling the NFM-P Database...
```

When the uninstallation is complete, the following is displayed:

```
Complete!
```

14

When the uninstallation is complete, enter the following to reboot the primary database station:

```
# systemctl reboot ↵
```

The station reboots.

15

Log in as the root user on the primary database station.

16

Open a console window.

17

Remove any files in the /opt/nsp/nfmp/db/tablespace and /opt/nsp/nfmp/db/archivelog directories.

18

Copy the database backup file set to the primary database station.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: The path to the backup file set must be the same as the path to the file set at creation time.

19

If you are restoring the database on a new station, for example, if the current primary database station is unusable, download or copy the following files for the installed NFM-P release to an empty directory on the database station:

- nsp-nfmp-jre-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-config-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-oracle-*R.r.p*-rel.*v*.rpm
- nsp-nfmp-main-db-*R.r.p*-rel.*v*.rpm
- OracleSw_PreInstall.sh

where

R.r.p is the NSP release identifier, in the form *MAJOR.minor.patch*

v is a version identifier

20

Navigate to the directory that contains the NFM-P installation files.

21

Enter the following:

```
# chmod +x * ↵
```

22

Enter the following:

```
# ./OracleSw_PreInstall.sh ↵
```

Note: The default values displayed by the script are shown as [*default*]. To accept a default value, press ↵.
The following prompt is displayed:

```
This script will prepare the system for a new install/restore of
an NFM-P Version R.r Rn database.
Do you want to continue? [Yes/No]:
```

23

Enter Yes. The following prompt is displayed:

```
Enter the Oracle dba group name [group]:
```

24

Enter a group name and press ↵.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: To reduce the complexity of subsequent software upgrades and technical support activities, it is recommended that you accept the default.

The following message is displayed:

```
Creating group group if it does not exist...
```

If you specify a new group, the following message is displayed:

```
done
```

25

If you specify an existing group, the following prompt is displayed:

```
WARNING: Group group already exists locally.
Do you want to use the existing group? [Yes/No]:
```

Perform one of the following.

a. Enter Yes ↵.

b. Enter No ↵. Go to Step 24 .

26

If the default user exists in the specified group, the following prompt is displayed:

```
The user [username] for the group [group] already exists locally.
Do you want to use the existing user? [Yes/No]:
```

27

Perform one of the following.

a. Enter Yes ↵; the following messages are displayed:

```
Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19...
Checking user username...
WARNING: Oracle user with the specified name already exists locally.
Redefining the primary group and home directory of user username ...
usermod: no changes
Changing ownership of the directory /opt/nsp/nfmp/oracle19 to
username:group.
About to unlock the UNIX user [username]
Unlocking password for user username
passwd: Success
Unlocking the UNIX user [username] completed
```

b. Enter No ↵. The following prompt is displayed:

```
Enter the Oracle user name:
```

Type a username and press ↵.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

The following messages and prompt are displayed:

```
Oracle user [username] new home directory will be
[/opt/nsp/nfmp/oracle19].

Checking or Creating the Oracle user home directory
/opt/nsp/nfmp/oracle19..

Checking user username...

Adding username...

Changing ownership of the directory /opt/nsp/nfmp/oracle19 to
username:group.

About to unlock the UNIX user [username]

Unlocking password for user username.

passwd: Success

Unlocking the UNIX user [username] completed

Please assign a password to the UNIX user username ..

New Password:
```

28

Perform one of the following.

a. If you specify a new user in Step 27 , the following prompt is displayed:

```
Please assign a password to the UNIX user username ..

New Password:
```

Perform the following steps.

1. Type a password and press ↵. The following prompt is displayed:

   ```
   Re-enter new Password:
   ```

2. Retype the password and press ↵. The following message is displayed if the password update is successful:

   ```
   passwd: password successfully changed for username
   ```

b. If you specify an existing user in Step 27 , the following prompt is displayed:

```
Do you want to change the password for the UNIX user username?
[Yes/No]:
```

Type No ↵.

29

The following prompt is displayed:

```
Specify whether an NFM-P server will be installed on this workstation.

The database memory requirements will be adjusted to account for the
additional load.

Will the database co-exist with an NFM-P server on this workstation
[Yes/No]:
```


© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Enter Yes or No, as required, and press ↵.

Messages like the following are displayed as the script execution completes:

```
INFO: About to set kernel parameters in /etc/sysctl.conf...
INFO: Completed setting kernel parameters in /etc/sysctl.conf...
INFO: About to change the current values of the kernel parameters
INFO: Completed changing the current values of the kernel parameters
INFO: About to set ulimit parameters in /etc/security/limits.conf...
INFO: Completed setting ulimit parameters in /etc/security/limits.
conf...
INFO: Completed running Oracle Pre-Install Tasks
```

30

When the script execution is complete, enter the following to reboot the database station:

```
# systemctl reboot ↵
```

The station reboots.

31

When the reboot is complete, log in as the root user on the primary database station.

32

Navigate to the directory that contains the NFM-P installation files.

33

Perform one of the following:

a. If you are restoring the database on the same station, enter the following:

```
# dnf install nsp-nfmp-main-db* ↵
```

b. If you are restoring the database on a new station, enter the following:

```
# dnf install *.rpm ↵
```

The dnf utility resolves any package dependencies, and displays the following prompt:

```
Total size: nn G
Installed size: nn G
Is this ok [y/d/N]:
```

34

Enter y. The following and the installation status are displayed as each package is installed:

```
Downloading packages:
Running transaction check
Running transaction test
Transaction test succeeded
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
Running transaction
```

The package installation is complete when the following is displayed:

```
Complete!
```

35

If you installed the Oracle RPM in the previous steps and the database backup was created while an NFM-P service pack that upgrades the Oracle software was applied, perform the following steps. Otherwise, go to Step 36.

1. Configure and apply the primary main database using samconfig -m db, as described in the *NSP Installation and Upgrade Guide*.
2. If the Oracle RPM must also be reinstalled on the standby database station, install the RPMs and configure and apply the standby main database using samconfig -m db, as described in the *NSP Installation and Upgrade Guide*.
3. Configure and apply the primary main server using samconfig -m main, as described in the *NSP Installation and Upgrade Guide*.
4. Apply the NFM-P service pack that matches the Oracle version of the database backup, as described in the service pack notice for the release.
5. Do not perform the remaining steps. Perform this procedure again to restore the database on the same station.

36

If the backup set is compressed as a tar file, you can obtain the absolute path of the database backup file set from the BACKUP_SUMMARY.INFO file. Perform the following to extract the BACKUP_SUMMARY.INFO file from the tar file:

```
# tar -xvf path BACKUP_SUMMARY.INFO
```

where *path* is the absolute path of the compressed database backup file

37

Perform one of the following.

a. If you are restoring the primary database on the same station, enter the following:

```
# samrestoreDb path ↵
```

where *path* is the absolute path of the directory that contains the database backup file set

b. If you are restoring the database on a new primary database station, enter the following:

```
# samrestoreDb path -standbyinstance instance -standbyip IP_address
↵
```

where

path is the absolute path of the directory that contains the database backup file set

instance is the standby database instance name

IP_address is the standby database IP address

The database restore begins.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

If the backup file set has been created using file compression, messages like the following are displayed.

```
About to uncompress backup files under path
Completed uncompressing backup files under path
```

Messages like the following are displayed as the restore progresses.

```
Restore log is /opt/nsp/nfmp/db/install/NFM-P_Main_Database.restore.
yyyy.mm.dd-hh.mm.ss.stdout.txt
<date time> working..
<date time> Performing Step 1 of 7 - Initializing ..
<date time> Executing StartupDB.sql ...
<date time> Performing Step 2 of 7 - Extracting backup files .....
<date time> Performing Step 3 of 7 - Restoring archive log files ..
<date time> Performing Step 4 of 7 - Executing restore.rcv ..........
<date time> Performing Step 5 of 7 - Restoring Accounting tablespaces
.......
<date time> Performing Step 6 of 7 - Opening database .....
<date time> working....
<date time> Executing ConfigRestoreDB.sql ...................
<date time> working..............
<date time> Performing Step 7 of 7 - Configuring SAM Server settings
...
```

The following is displayed when the restore is complete:

```
<date time> Database restore was successful
DONE
```

38

When the database restore is complete, close the console window.

39

Log in to the primary main server station as the root user.

40

Enter the following to enable the automatic main server startup:

```
# systemctl enable nfmp-main.service ↵
```

41

Start the primary main server.

1. Enter the following to switch to the nsp user

   ```
   # su - nsp ↵
   ```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↵
   ```

4. Enter the following to display the server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully initialized if the status is the following:

   ```
   Application Server process is running.  See nms_status for more
   detail.
   ```

   If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

42

Perform a full resynchronization of the network to discover the interim changes in the managed network.

43

Start the standby database.

1. Log in to the standby main database station as the root user.
2. Enter the following to start the Oracle proxy:

   ```
   # systemctl start nfmp-oracle-proxy.service ↵
   ```

3. Enter the following to start the database:

   ```
   # systemctl start nfmp-main-db.service ↵
   ```

44

Log in to the standby main server station as the root user.

45

Enter the following to enable the automatic main server startup:

```
# systemctl enable nfmp-main.service ↵
```

46

Start the standby main server.

1. Enter the following to switch to the nsp user

   ```
   # su - nsp ↵
   ```

2. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

3. Enter the following:

   ```
   bash$ ./nmsserver.bash start ↵
   ```

4. Enter the following to display the server status:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
bash$ ./nmsserver.bash appserver_status ↵
```

The server status is displayed; the server is fully initialized if the status is the following:

```
Application Server process is running.  See nms_status for more
detail.
```

If the server is not fully initialized, wait five minutes and then repeat this step. Do not perform the next step until the server is fully initialized.

47

To restore the database redundancy, reinstantiate the primary database on the standby database station, as described in 22.20 “How do I reinstantiate the main database from the client GUI?” (p. 755) or 22.21 “How do I reinstantiate the main database from a CLI?” (p. 756).

END OF STEPS

22.17 How do I delete the inactive residential subscriber instances?

22.17.1 Purpose

It is recommended that you periodically remove the inactive subscriber instance records from the NFM-P main database. A subscriber instance becomes inactive when the associated subscriber is deleted from an NE. The inactive instances accumulate rapidly, for example, in a Wi-Fi offload deployment.

Perform this procedure to configure and execute a script that removes the inactive subscriber instance records from the main database.

Note: Before you perform the procedure, it is recommended that you disable the GUI client timeout so that you can use the client GUI to monitor the script execution. Otherwise, if the execution takes longer then the GUI client timeout, you can monitor the script execution using the NFM-P user activity log.

22.17.2 Steps

Disable GUI client timeout

1

Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security — Security Management (Edit) form opens.

2

Set the Client Timeout (minutes) parameter to 0, which specifies no timeout.

3

Save your changes and close the form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Configure a script bundle

4

Choose Tools→Scripts from the NFM-P main menu. The Scripts form opens.

5

Choose Script Bundle (Scripting) from the drop-down menu and click Search. A list of script bundles is displayed.

6

If a subscriber instance deletion script bundle is listed, go to Step 12.

7

Click Browse Examples. The Browse Examples of Scripts form opens.

8

Navigate to the required bundle example. The path is Script Bundle Examples→Miscellaneous→Remove Inactive Residential Subscriber Instances Bundle.

9

Select the bundle example and click Create Bundle. The Script Bundle (Create) form opens.

10

Configure the Name parameter.

11

Save your changes and close the forms.

Execute the script bundle

12

Select the script bundle in the Scripts form and click Properties. The Script Bundle (Edit) form opens.

13

Select Remove Residential Subscriber CTL and click Execute Script. The Execute Script form opens.

14

Configure the parameter on the form to specify the number of days of inactivity that qualify a subscriber instance for deletion.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: If the NFM-P forwards statistics or billing information to NSP Analytics, ensure that the parameter value is greater than the billing period in days to ensure that no inactive subscriber instances are deleted before the billing occurs.

15

Click Execute. The script execution begins.

While the script runs, a new item with an hourglass symbol is displayed in the navigation panel on the left side of the form. When the script execution is complete, the symbol changes to a green check mark.

16

Close all forms.

17

If required, restore the GUI client timeout to its original value.

END OF STEPS

22.18 How do I export an NFM-P main database?

22.18.1 Purpose

Perform this procedure to export the main database content to a file set.

You require the following user privileges:

- on each main server station — root
- on the standalone or primary main database station:
  - root
  - Oracle database user — password initially set as the user-password value in the database section of samconfig
  - Oracle management user — user name specified during database installation; default is ‘oracle’
  - Oracle SYS user — default password available from technical support

CAUTION

Service Disruption

A database export operation requires a shutdown of each main server, which causes a network management outage.

You must perform this procedure only during a scheduled maintenance period.

Note: The passwords that you enter in the procedure are not displayed.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.18.2 Steps

General preparation

1

Clear all outstanding failed deployments. See “To view and manage failed deployments” in the *NSP NFM-P Classic Management User Guide* for information about how to clear a failed deployment.

2

Obtain the following main database information; in a redundant deployment, you require the primary database information:

- Oracle database instance name—default is samdb1
- Oracle database user password—set initially as the user-password value in the database section of samconfig on the standalone or primary main server
- Oracle SYS user password—default available from technical support

Stop main servers

3

Perform the following steps on each main server station to stop the main server.

Note: In a redundant deployment, you must stop the standby main server first.

1. Log in to the main server station as the nsp user.
2. Open a console window.
3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↲
   ```

4. Enter the following to stop the main server:

   ```
   bash$ ./nmsserver.bash stop ↲
   ```

5. Enter the following to display the main server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↲
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Run database export script

4

Log in to the main database station as the Oracle management user.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

5

Open a console window.

6

If the directory that is to hold the database export file set does not exist, create the directory.

Note: The database export operation fails if the directory that is to contain the exported database file set does not exist.
The directory must be a directory on the local file system to which the Oracle management user has read/write access.

7

Enter the following:

```
bash$ /opt/nsp/nfmp/db/install/config/samdb/SAMDb_exportImport.sh -e destination ↵
```

where *destination* is the absolute path of the directory that is to hold the database file set

Note: To display the script usage, specify the -h option, as follows:
SAMDb_exportImport.sh -h ↵

The following messages and prompt are displayed:

```
Using DB_INSTALL_BASE = /opt/nsp/nfmp/db/install
Using ORACLE_SID = maindb1
Using ORACLE_HOME = /opt/nsp/nfmp/oracle19
Enter the password for the "sys" user (terminal echo is off):
```

8

Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
Enter the password for database_user (terminal echo is off):
```

9

Enter the Oracle database user password and press ↵.

The following prompt is displayed:

```
Enter the export encryption password (terminal echo is off):
```

10

Create and record a database export encryption password. The password is required for a subsequent database import operation.

Note: The password can be of any length and use any characters.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

11

Type the created password and press ↵.

The following prompt is displayed:

```
Confirm export encryption password (terminal echo is off):
```

12

Retype the password and press ↵.

The following message and prompt are displayed:

```
This tool will shutdown the db listener disconnecting any connections
to the database.
Have the SAM servers been shutdown? [y/n/q] (y):
```

13

Press ↵.

The following message and prompt are displayed:

```
To optimize the speed of the export this script will use as many CPUs
as you allow it to.
The maximum number of CPUs available are n
How many CPUs will be used for this export? (1):
```

14

Type the number of CPUs to use for the export operation, and press ↵.

The following prompt is displayed:

```
Do you want to perform an export size estimate first? [y/n/q] (y):
```

15

Press ↵ to direct the script to estimate the amount of disk space that the export requires.

The script displays an estimate of the required disk space, the available space in the partition that contains the destination directory, and the following prompt:

```
Do you have enough space? [y/n/q] (n):
```

16

Perform one of the following.

a. Confirm the space requirement and proceed with the export.
   1. Type y ↵ if the partition has sufficient capacity to hold the exported file set.

      The following prompt is displayed:

      ```
      Proceed with the export? [y/n/q] (y):
      ```

   2. Press ↵. The database export begins.

      The script displays information that includes the export log filename and a series of progress indicators.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

b. Press ↵ if the partition lacks sufficient capacity to hold the exported file set.

The following message is displayed and the script exits:

```
Cancelling export...
```

17

Close the open console windows, as required.

END OF STEPS

22.19 How do I import an NFM-P main database?

22.19.1 Purpose

Perform this procedure to import a main database from an exported file set.

You require the following user privileges:

- on each main server station — root
- on the standalone or primary main database station:
  - root
  - Oracle database user — password initially set as the user-password value in the database section of samconfig
  - Oracle management user — user name specified during database installation; default is 'oracle'
  - Oracle SYS user — default password available from technical support

CAUTION

Service Disruption

A database import operation requires a shutdown of each main server, which causes a network management outage.

You must perform this procedure only during a scheduled maintenance period.

Note: The passwords that you enter in the procedure are not displayed.

22.19.2 Steps

Stop main servers

1

Perform the following steps on each main server station to stop the main server.

Note: In a redundant deployment, you must stop the standby main server first.

1. Log in to the main server station as the nsp user.
2. Open a console window.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

3. Enter the following:

   ```
   bash$ cd /opt/nsp/nfmp/server/nms/bin ↵
   ```

4. Enter the following to stop the main server:

   ```
   bash$ ./nmsserver.bash stop ↵
   ```

5. Enter the following to display the main server status:

   ```
   bash$ ./nmsserver.bash appserver_status ↵
   ```

   The server status is displayed; the server is fully stopped if the status is the following:

   ```
   Application Server is stopped
   ```

   If the server is not fully stopped, wait five minutes and then repeat this step. Do not perform the next step until the server is fully stopped.

Install database

2

You can perform a main database import only on a station that has a newly installed main database; perform one of the following.

a. If the station on which you are performing the import hosts a main database that is not newly installed, uninstall the database, as described in the *NSP Installation and Upgrade Guide*.

b. If the station on which you are performing the import has no main database installed, install a main database on the station, as described in the *NSP Installation and Upgrade Guide*.

Run database import script

3

Copy the exported database file set to the database station.

Note: The directory to which you copy the file set must contain no other files. The directory must be a directory on the local file system to which the Oracle management user has read/write access.

4

Log in to the database station as the Oracle management user.

5

Open a console window.

6

Enter the following:

```
bash$ /opt/nsp/nfmp/db/install/config/samdb/SAMDb_exportImport.sh -i source ↵
```

where *source* is the absolute path of the directory that contains the exported database file set

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Note: To display the script usage, specify the -h option, as follows:
SAMDb_exportImport.sh -h ↵

The following messages and prompt are displayed:

```
Using DB_INSTALL_BASE = /opt/nsp/nfmp/db/install
Using ORACLE_SID = maindb1
Using ORACLE_HOME = /opt/nsp/nfmp/oracle19
Enter the password for the "sys" user (terminal echo is off):
```

7

Enter the Oracle SYS user password and press ↵.

The following prompt is displayed:

```
Enter the password for database_user (terminal echo is off):
```

8

Enter the Oracle database user password and press ↵.

The following prompt is displayed:

```
Enter the export encryption password (terminal echo is off):
```

9

Enter the database export encryption password created during the database export operation.

The following messages and prompt are displayed:

```
In order to optimize the speed of this import, this script needs to
know how many CPUs are available on this machine and how many data
files there are to import.
This machine appears to have n CPUs
Is this correct? [y/n/q] (y):
```

10

Type the number of CPUs to use for the export operation, and press ↵.

The following message and prompt are displayed:

```
There appears to be n data files to import   Is this correct? [y/n/q]
(y):
```

11

Press ↵ if the number of data files to import is correct.

The following message and prompt are displayed:

```
Log of import command will be written to log_file
Proceed with the import? [y/n/q] (y):
```

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

12

Press ↵ to proceed with the database import.

The script generates messages like the following as it begins to import the database.

```
Adding addition datafiles to existing tablespacesRestore wallet file
Restarting the database...
Shutting down the listener
Starting import: timestamp
```

where *timestamp* is the start time of the import operation

The script displays a series of progress indicators.

The following messages are displayed when the import operation is complete:

```
Executing recreate TI_BULK* packages body
Import done: timestamp
Starting up the listener
Here is the import log: log_file
```

where

log_file is the name of a log file that the script creates

timestamp is the start time of the import operation

13

Close the open console windows, as required.

END OF STEPS

22.20 How do I reinstantiate the main database from the client GUI?

22.20.1 Purpose

Perform this procedure to use the NFM-P GUI to restore the main database redundancy in a redundant NFM-P system by reinstantiating the primary main database on the standby database station. Database reinstantiation is required after a main database failure.

If automatic database reinstantiation is enabled, a failed manual reinstantiation attempt does not affect the reinstantiation timer. If a manual reinstantiation is successful, the NFM-P does not attempt a subsequent reinstantiation.

Before you attempt to perform this procedure, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the primary main server.
- The database listener is operating.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

22.20.2 Steps

1

Log in to a GUI client as a user that has an assigned Administrator scope of command role.

2

Choose Administration→System Information from the NFM-P main menu. The System Information form opens.

3

If you are performing this procedure after a database failover or switchover, ensure that the Failover State or Switchover State on the form is Successful.

Note: The state must read Successful before you can continue.

4

Click Re-Instantiate Standby, and then click Yes. The database reinstantiation begins.

Note: The Re-Instantiate Standby button is displayed only if your user account has an appropriate scope of command.

The client GUI status bar and the System Information form display the reinstantiation status. The Standby Re-instantiation State changes from In Progress to Success when the reinstantiation is complete. The Last Attempted Standby Re-instantiation Time displays the start time of the current reinstantiation.

5

When the reinstantiation is complete, close the System Information form.

6

View the NFM-P GUI status bar to verify that the NFM-P main servers and main database are communicating and operational.

END OF STEPS

22.21 How do I reinstantiate the main database from a CLI?

22.21.1 Purpose

Perform this procedure to use a CLI to restore the main database redundancy in a redundant NFM-P system by reinstantiating the primary main database on the standby database station. Database reinstantiation is required after a main database failure.

If automatic database reinstantiation is enabled, a failed manual reinstantiation attempt does not affect the reinstantiation timer. If a manual reinstantiation is successful, the NFM-P does not attempt a subsequent reinstantiation.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Before you attempt to perform this procedure, the following conditions must be true:

- The primary database proxy and the standby database proxy are in contact with the primary main server.
- The database listener is operating.

Note: You require nsp user privileges on the primary main server station.

22.21.2 Steps

1

Log in to the primary main server station as the nsp user.

2

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4

Enter the following:

```
bash$ ./reinstantiatedb.bash -u username -p password ↵
```

where

username is the name of an NFM-P user account that has an assigned Administrator scope of command role

password is the password for the user account

The following prompt is displayed:

```
This action will rebuild the standby database.
Do you want to proceed? (YES/no) :
```

5

Enter the following:

```
YES ↵
```

The NFM-P begins to reinstantiate the main database on the standby main database station. Progress is indicated by a rolling display of dots in the console window. The reinstantiation is complete when the CLI prompt reappears.

6

When the reinstantiation is complete, close the console window.

7

Open an NFM-P GUI client.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

8

View the NFM-P GUI status bar to verify that the NFM-P main servers and main database are communicating and operational.

END OF STEPS

22.22 How do I regenerate NSP TLS certificates for an NFM-P database?

22.22.1 Purpose



CAUTION

Service Disruption

Performing the procedure requires that you shut down the NFM-P database, which may be service-affecting.

If the database is in service, ensure that you perform the procedure only during a scheduled maintenance period.

This procedure describes how to regenerate TLS certificates from the NSP cluster for an NFM-P database. Perform this procedure on a primary, standby, or standalone database.

22.22.2 Steps

1

Depending on the role of the database you are updating, complete one of the following substeps:

a. If you need to update only the primary database, stop the NFM-P main servers, standby database, and any auxiliary servers. Then proceed to Step 2.

b. If you need to update a standalone server, you must shut down the NFM-P main server and any auxiliary servers before proceeding to Step 2.

c. If you need to update only the standby database, you do not need to shut down the NFM-P main server or any other components; proceed to Step 2.

Procedure references for above server actions:

- 21.3 “How do I stop a main server?” (p. 593)
- 21.5 “How do I stop a main database?” (p. 595)
- 21.7 “How do I stop an auxiliary server?” (p. 597)

2

Log in as the root user on the database station.

3

Open a console window and enter the following:

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

```
# samconfig -m db ↲
# configure tls ↲
# regenerate-certs ↲
# exit ↲
# apply ↲
```

4

Restart the NFM-P main server and any other stopped components, referring to the following procedures:

- 21.2 “How do I start a main server?” (p. 593)
- 21.4 “How do I start a main database?” (p. 594)
- 21.6 “How do I start an auxiliary server?” (p. 596)

END OF STEPS

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

A Remote authentication sample configurations

A.1 Remote authentication server configurations

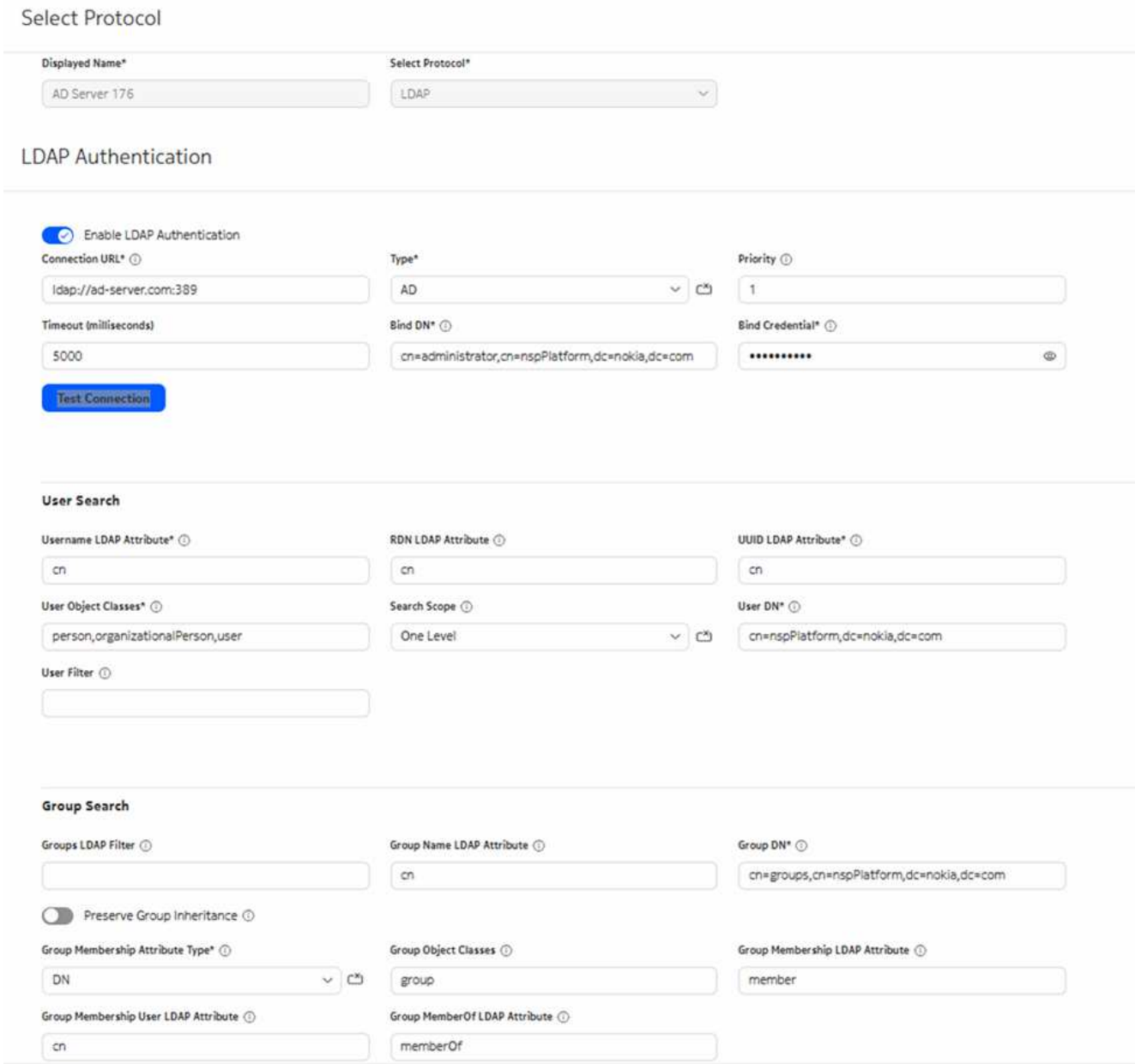
A.1.1 Purpose

This appendix provides sample configurations for remote authentication servers and identity providers.

A.1.2 Sample Active Directory server configuration

The following example is an Active Directory authentication server configuration, as it appears in the NSP Users and Security Settings, Create Server form.

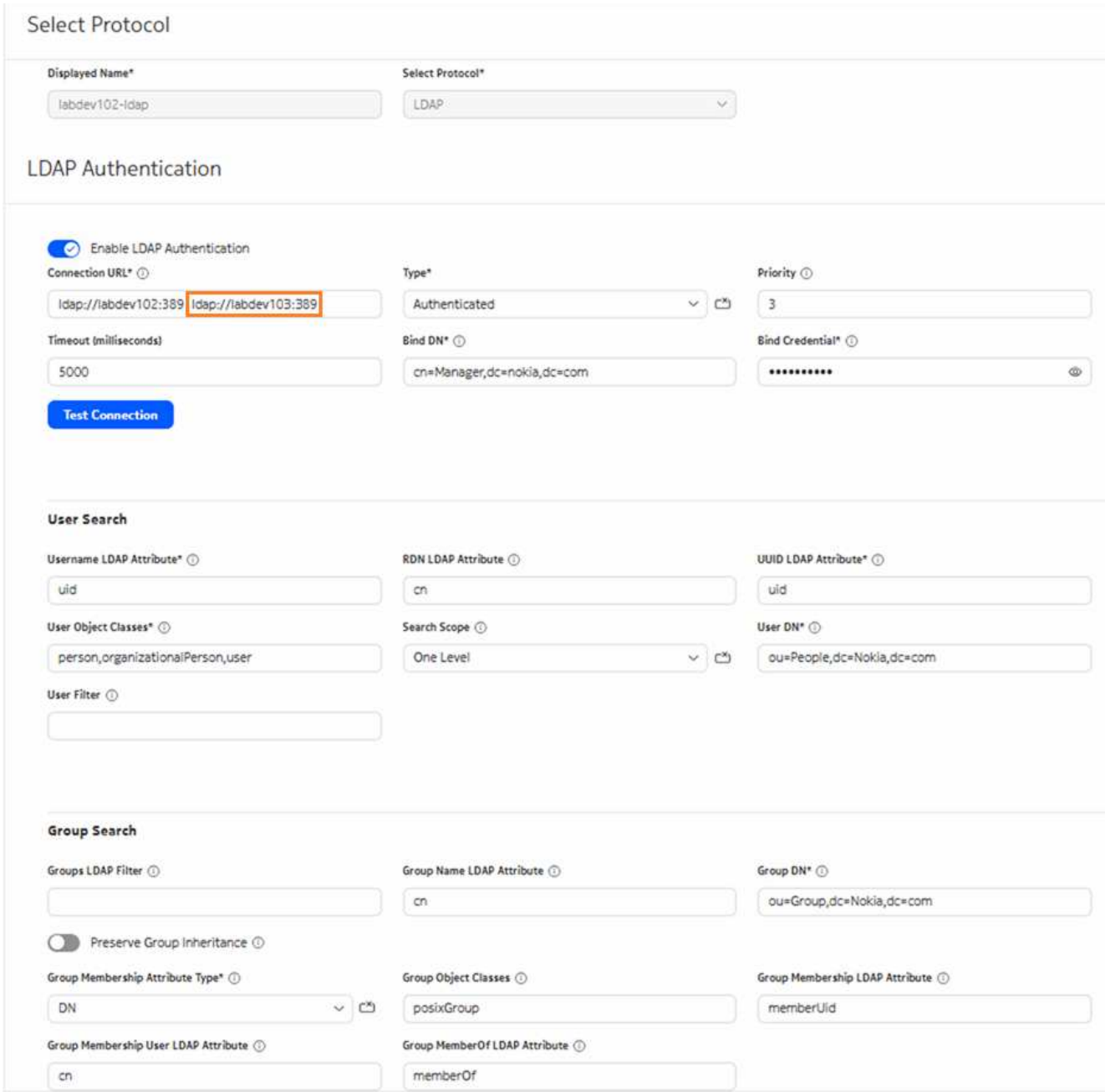
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



A.1.3 Sample LDAP server configuration

The following example is an LDAP authentication server configuration, as it appears in the NSP Users and Security Settings, Create Server form. This configuration includes an optional redundant server URL (highlighted).

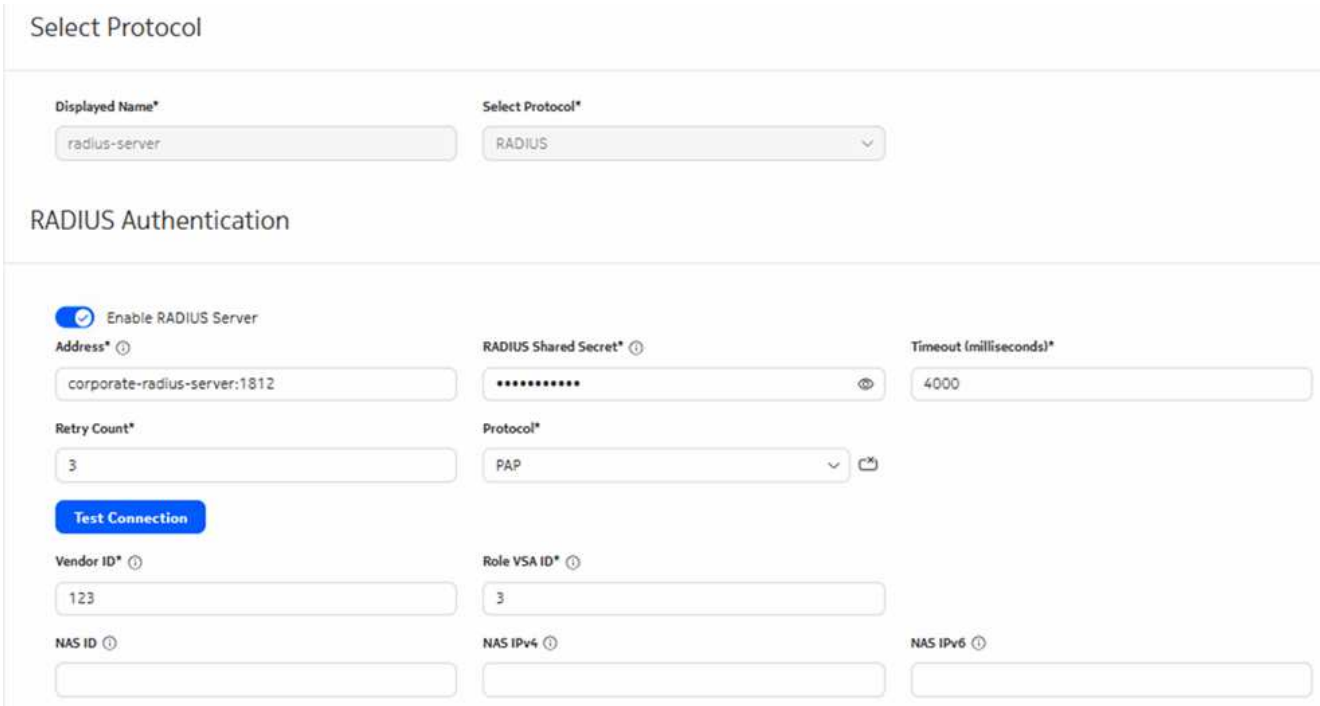
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



A.1.4 Sample RADIUS server configuration

The following example is a RADIUS authentication server configuration, as it appears in the NSP Users and Security Settings, Create Server form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

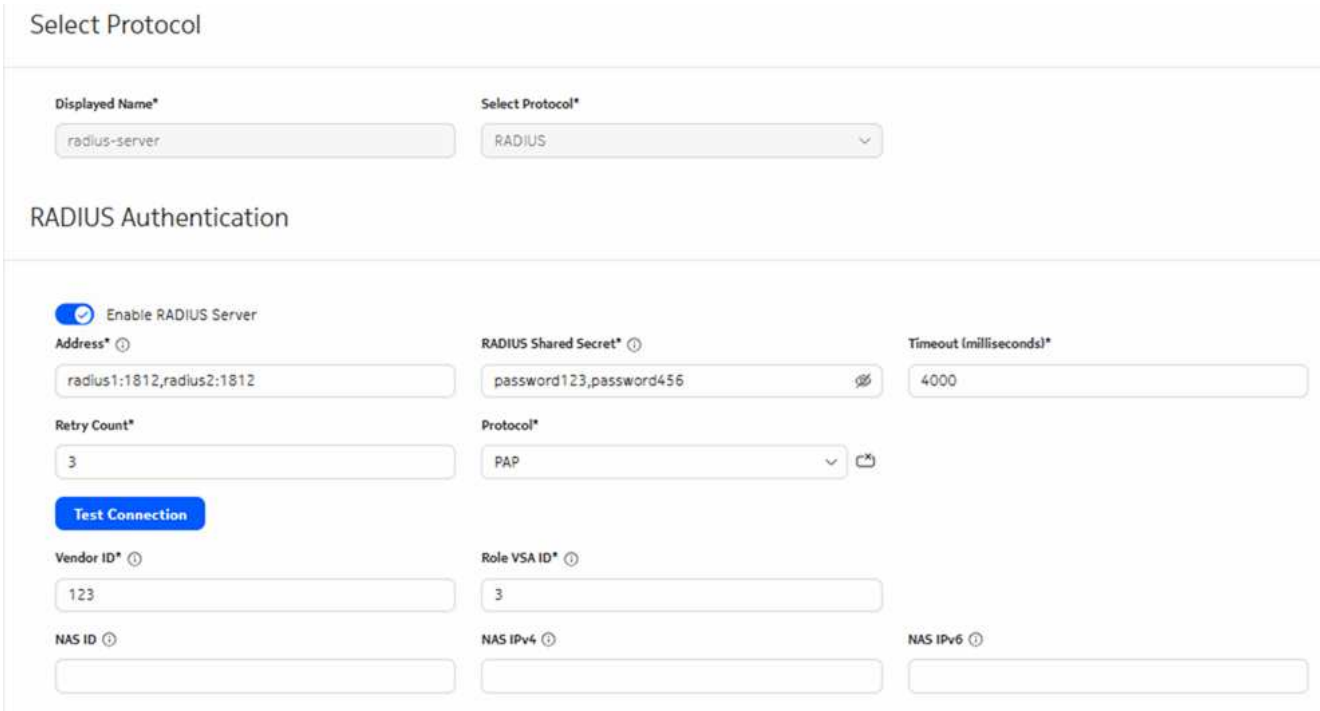


A.1.5 Sample configuration for two RADIUS servers

The following example is a double RADIUS authentication server configuration, as it appears in the NSP Users and Security Settings, Create Server form.

Note how two comma-separated RADIUS server addresses are specified in the Address field, and two comma-separated passwords are specified in the RADIUS Shared Secret field

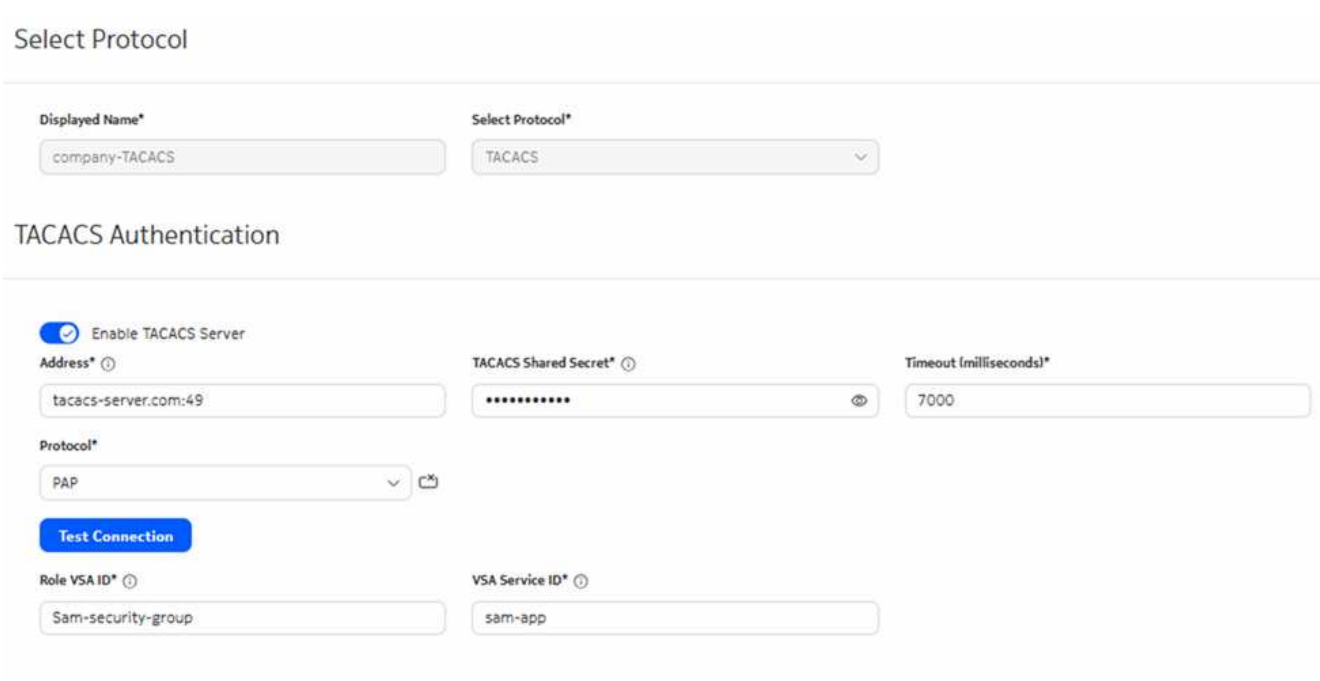
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



A.1.6 Sample TACACS server configuration

The following example is a TACACS authentication server configuration, as it appears in the NSP Users and Security Settings, Create Server form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

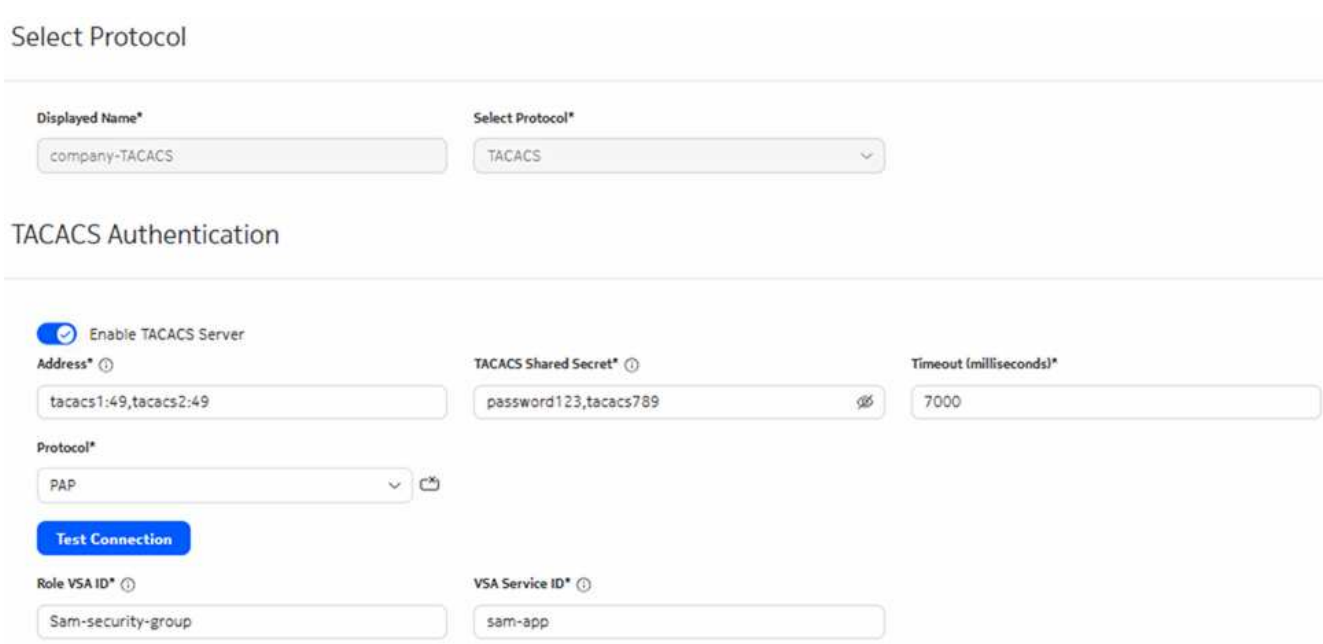


A.1.7 Sample configuration for two TACACS servers

The following example is a double TACACS authentication server configuration, as it appears in the NSP Users and Security Settings, Create Server form.

Note how two comma-separated TACACS server addresses are specified in the Address field, and two comma-separated passwords are specified in the TACACS Shared Secret field

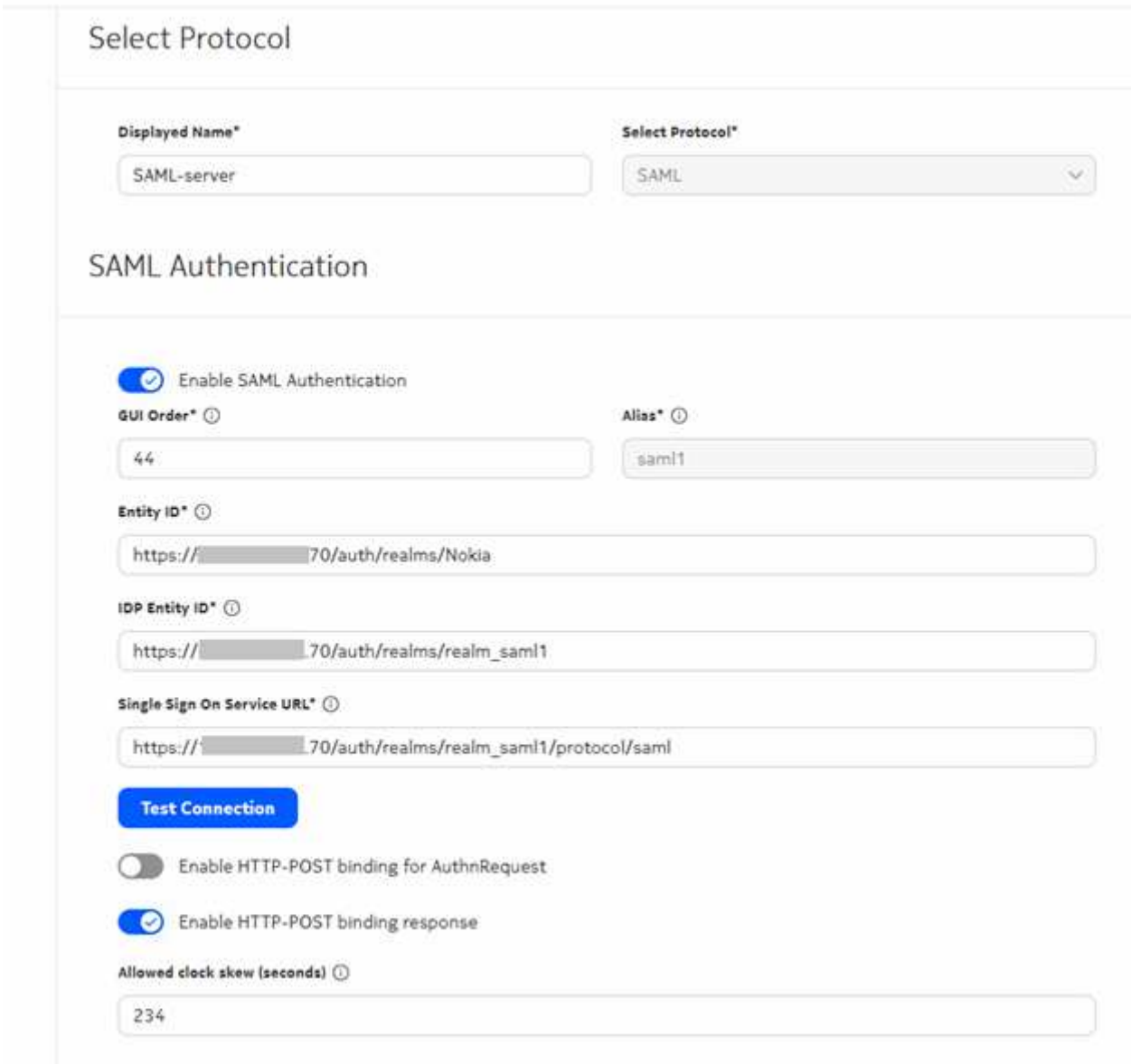
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



A.1.8 Sample SAML server configuration

The following example is a SAML identity provider configuration, as it appears in the NSP Users and Security Settings, Create Server form.

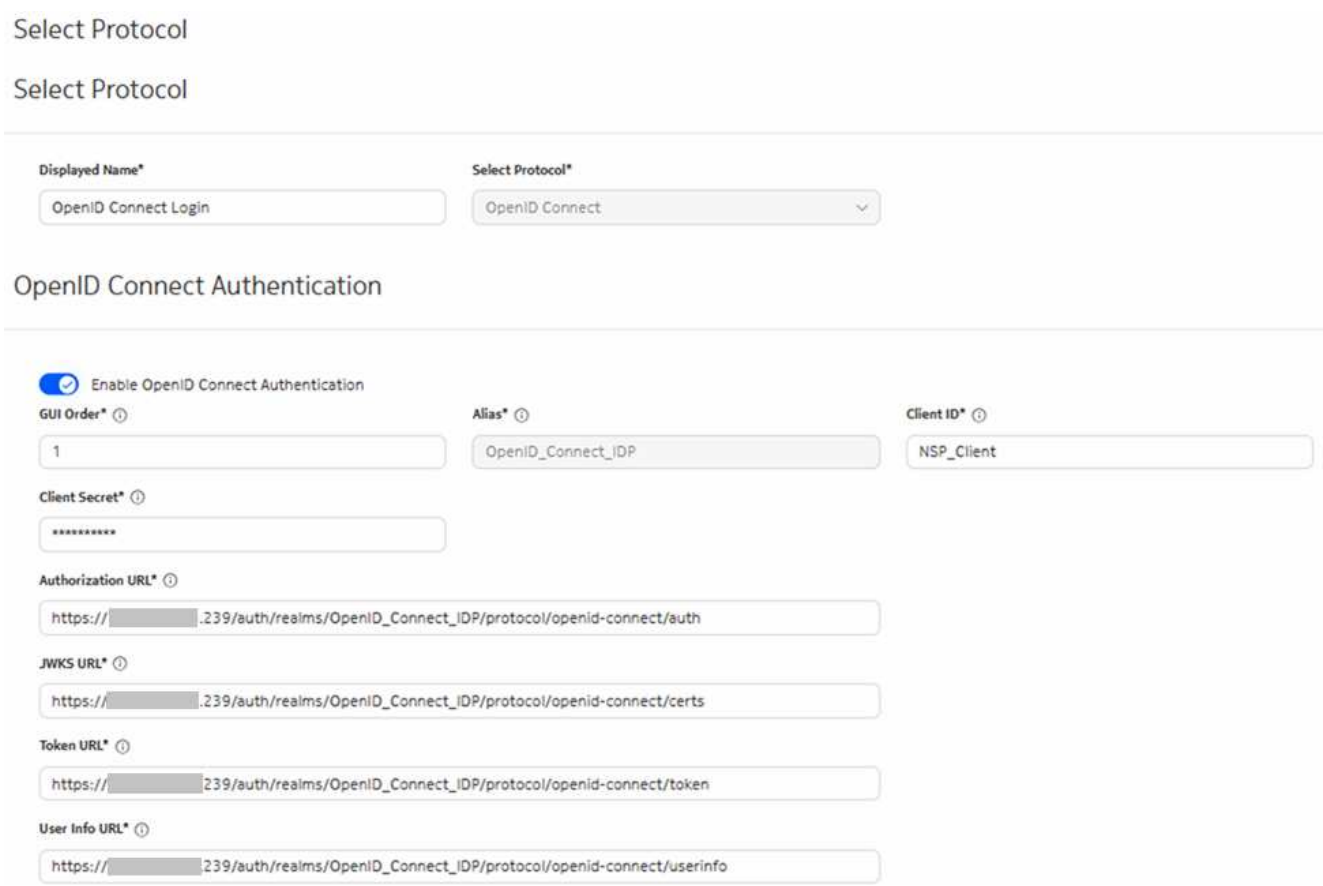
© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



A.1.9 Sample OIDC server configuration

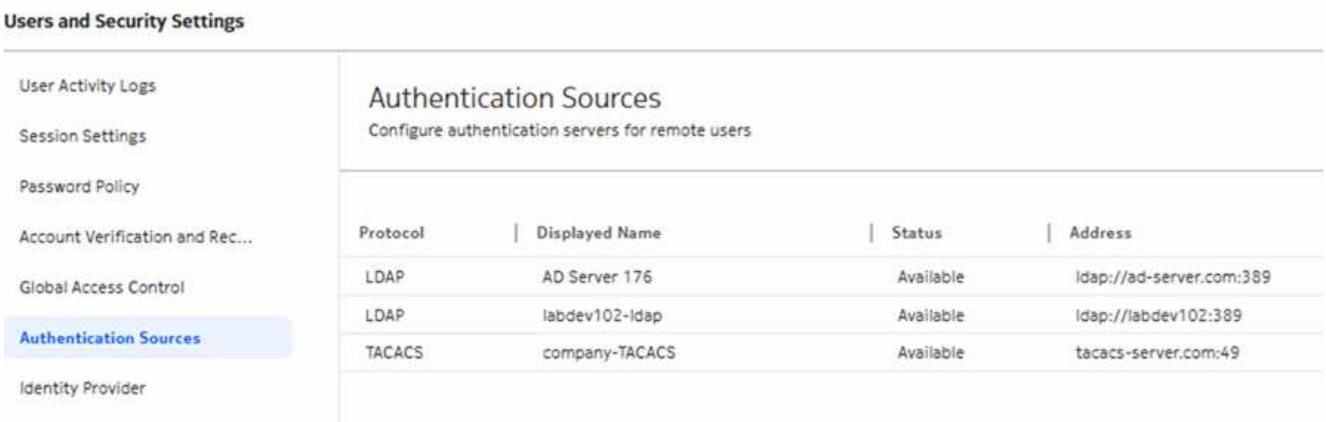
The following example is an OpenID Connect identity provider configuration, as it appears in the NSP Users and Security Settings, Create Server form.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms



A.1.10 Authentication Sources configuration

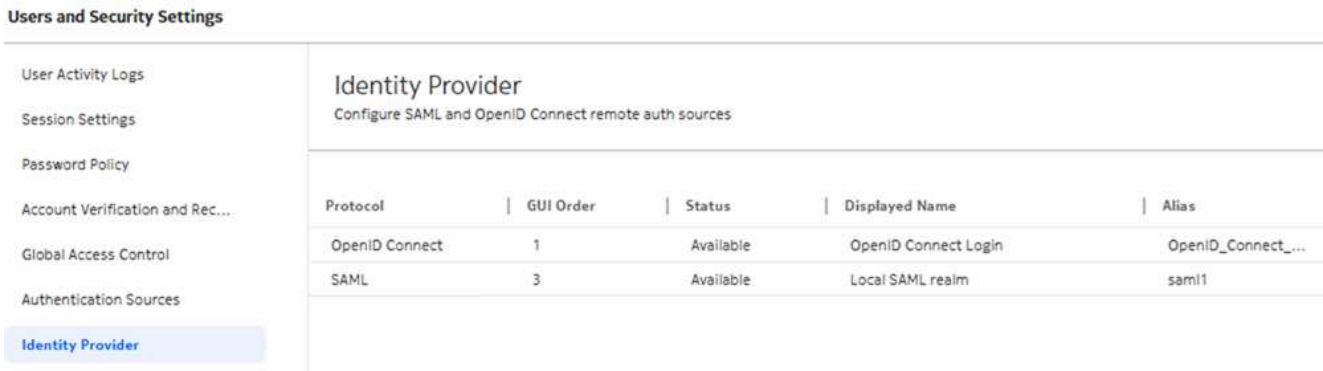
Configured authentication servers, as they appear in the NSP Users and Security Settings, Authentication Sources list.



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

A.1.11 Identity Providers configuration

Configured identity providers, as they appear in the NSP Users and Security Settings, Identity Providers list.



© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

B Classic management scope of command roles and permissions

B.1 What are the predefined NFM-P scope of command profiles and roles?

B.1.1 General information

This appendix describes the predefined NFM-P scope of command profiles and roles, and the access permissions for each predefined role. Predefined scope of command profiles and roles cannot be deleted.

Table B-1 Summary of command profiles, roles, and permission information

Table	Description
Table B-2, “Predefined scope of command profiles” (p. 771)	Lists the predefined scope of command profiles, the assigned roles for each profile, and a description for each profile.
Table B-3, “Predefined scope of command roles” (p. 771)	Lists the NFM-P predefined scope of command roles and provides a description of the user security access provided for each role.
B.2 “What are the permissions assignable to NFM-P scope of command roles?” (p. 774)	Lists the permissions that can be assigned to an NFM-P scope of command role and a description of the permission.
B.3 “What is the permissions access for NFM-P scope of command roles?” (p. 798)	Describes the access levels that can be assigned for permissions in a scope of command role, and how to view the permission configuration of a role.

B.1.2 Predefined scope of command profiles

Table B-2 Predefined scope of command profiles

Profile name	Assigned roles	Description
admin	Administrator	Default administrative scope of command profile with access to all menus accessible from the NFM-P GUI with the exception of LI menu functions. This profile also has no XML API access.

B.1.3 Predefined scope of command roles

Table B-3 Predefined scope of command roles

Role	Access provided
Base Read-only	Read-only to all objects except for the objects in the NFM-P Security and Mirror Service Management roles.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-3 Predefined scope of command roles (continued)

Role	Access provided
Administrator	GUI access, but no XML API access, to all objects. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
User Management	NFM-P user and group management. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
NFM-P Management and Operations	Database functions such as backup, restore, reinstantiation, and switchover. Alarm administration such as acknowledgement, clearing, and setting severity-change thresholds. General NE management functions such as discovery, deployment, mediation, polling, statistics management, and security management that includes modifying spans. Create, modify, delete, import, and export public workspaces. View private or public workspaces in the Manage Workspaces list.
Network Element Equipment Management	Physical equipment configuration and management.
Service Management	Service, service component, and service template management functions, excluding mirror-service management.
Old Service Template Management	Management of service templates deprecated; see Template Script Management in this table.
Subscriber Management	Customer and residential subscriber management.
QoS/ACL Policy Management	General QoS and ACL policy management, Ethernet service and time of day suite policy management.
Policy Management (except QoS/ACL)	Management of policies other than those in the QoS/ACL Policy Management role.
Routing Management	Routing protocol, L2 forwarding, and bandwidth management.
Tunnel Management	Service tunnel and underlying transport management.
NFM-P Management and Operations	Database management (Backups, Reinstantiation, and Switchovers), Alarm acknowledgement, Alarm clearing, and Severity Change Thresholds, Router administration (Scheduling, Backup Policies, Upgrade Policies, Deployment Policies, and Management Ping Policies), NE Security, LPS, and Mediation Policies, SNMP Poller/Stats Polices, Event Notification Policies, MIB Policies, SNMP Performance Statistics, Server Performance Statistics, Statistics Plotter, Usage and Activity Records, and Span configuration.
Network Element Software Management	NE software management functions.
Fault Management	Functions such as alarm management and remote network monitoring.
Service Test Management	STM functions such as creating, running and scheduling OAM tests.
Script Management	XML API and CLI script management, excluding execution.
Script Execution	XML API and CLI script execution.
Mirror Service Management	Creation and management of mirror services and mirror-service components using the GUI.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-3 Predefined scope of command roles (continued)

Role	Access provided
XML API Management	Use of the XML API.
Telnet/SSH Management	Telnet or SSH access to NEs from the GUI.
CPAM Management	Route Analysis of ISIS Topology, OSPF Topology, MPLS Topology, IP Path monitoring, LSP Monitoring, Checkpoints, and Impact Analysis Scenarios for CPAM management.
CPAM OSS PCA	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM routing.
CPAM Topology Simulator	Route Analysis of ISIS Topology, OSPF Topology, and MPLS Topology for CPAM Topology Simulator.
Root Cause Analysis (RCA) Object Verification	RCA functions.
Lawful Interception Management	LI configuration for mirror services, mediation policies, and NE security.
Template Script Management	Service and tunnel template script management.
Service Template Script Execution	Service template script execution.
Tunnel Template Script Execution	Tunnel template script execution.
Format and Range Policy Management	Format and range policy management, service-creation span rules.
Work Order Activation	The ability to perform CM work order activation.
Configuration Snapshot Export	The ability to perform export CM configuration snapshots.
Configuration Management which causes node reset	The ability to configure objects which causes a full or partial reset of the node.
EPC Operator	Read and write permission on all Evolved Packet Core classes.
Statistics Plotter Profile Management	Management of all Statistics Plotter profiles.
Admin Neto Launch	The ability to open the NEtO with the administration profile.
Viewer Neto Launch	The ability to open the NEtO with the viewer profile.
Default Neto Launch	The ability to open the NEtO with the null profile.
Ageout Constraint Policy Management	The ability to configure Ageout Constraint Policies.
Purge Records	The ability to purge historical records from the NFM-P such as statistics logs, event logs, etc.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

B.2 What are the permissions assignable to NFM-P scope of command roles?

B.2.1 Permissions assignable to NFM-P scope of command roles

Table B-4 Permissions assigned to NFM-P scope of command roles

Package.Class.Method/Property	Description
aaa	AAA - Configurations for authentication, authorization, and accounting.
aaa.RadiusProxyInterface	RADIUS Proxy Interface - Access to Radius Proxy Interface configuration.
aaa.RadiusProxyServer	RADIUS Proxy Server - Access to Radius Proxy Server configuration.
aaa.RadiusServer	RADIUS Server - Access to Radius Server configuration.
aapolicy.DbInfoTransitSubscriberManager.property_ dbInfoTransIpAddrRtrvTimeOut	Db Info Transit Subscriber Manager - property_ dbInfoTransIpAddrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
aapolicy.DbInfoTransitSubscriberManager.property_ dbInfoTransPrfxAddrRtrvTimeOut	Db Info Transit Subscriber Manager - property_ dbInfoTransPrfxAddrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
aapolicy.DbInfoTransitSubscriberManager.property_ dbInfoTransSubscrRtrvMax	Db Info Transit Subscriber Manager - property_ dbInfoTransSubscrRtrvMax - Service preferences can only be modified by a user with an administrator role.
accessuplink	Access Uplink - Configuration of 7210 Access Uplink Specifics for physical ports and LAG interfaces.
accounting	Accounting Policy - Statistics Accounting Policies.
aclfilter	ACL Filter Policy - MAC, IP, and IPv6 ACL Filters.
aclfilterli	ACL Filter LI - All configurations for mirroring of packets matching entries of Lawful intercept ACL filters to mirror destinations.
activation	Activation - Used to define, manage, and deploy work orders used in activation.
activation.Session	Activation Session - Used to manage activation sessions and activate work orders.
activation.Snapshot	Snapshot - Used to manage CM configuration snapshots.
activation.SnapshotEntity	Snapshot Entity - Used to manage snapshot entities.
activation.WebDAVSharedData	activation.WebDAVSharedData - Ability to restrict access to CM data (CM work orders and configuration snapshots) via the WebDAV protocol.
activation.WorkOrder	Work Order - Used to manage work orders.
aengr	Access Egress Policy - Access Egress QoS Policies.
ageoutcstr	Ageout Constraint - Configurations related to Ageout Constraint.
aggregator	Aggregation - Aggregation Manager.
aingr	Access Ingress Policy - Access Ingress QoS Policies.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
analytics	Analytics - Analytics Manager.
ancp	ANCP - Access Node Control Protocol (ANCP) policy and configuration.
ancp.AncpLoopback	ANCP Loopback - Access to ANCP Loopback tests, ANCP Loopback test definitions, and ANCP Loopback deployed tests.
antispoof	Anti-Spoofing - Anti-Spoofing for L2/L3 Access Interfaces and Filter configuration.
aosqos	AoS QoS - Quality of Service for Application over Signaling (AoS QoS) Policy and conditions, AoS QoS configuration for Physical Port and Layer 2 Bridge.
aosredundancy	Aos-Redundancy - AOS Multichassis.
aossas	AOS SAS - OAM tests specific to AOS nodes.
aossas.CPETestGroupHead	CPE SLA Test Group - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
aossas.CPETestHead	CPE SLA Test - Access to CPE SLA tests, CPE SLA test definitions, and CPE SLA deployed tests.
apipe	APipe - All contained objects are listed. Package access is not currently used.
apipe.Apipe	Apipe Service - Access to VLL ATM Pipe (Apipe) Service objects themselves.
apipe.Site	Apipe Site - Access to Apipe Sites.
aps	APS - Automatic Protection Switching (APS) Groups.
arp	ARP - ARP host and configurations on service interfaces.
assurance	Assurance - Parent package for all Assurance event classes.
atm	ATM - ATM configuration for Service interfaces and routers, ATM Connections, ILMI Link, and other ATM related objects.
atm.AtmPing	ATM Ping - Access to ATM Ping tests, ATM Ping test definitions, and ATM Ping deployed tests.
atmpolicy	ATM QoS Policy - ATM Traffic Descriptor Policy.
audit	Resource Audit - Ability to execute audits and view audit results.
autoconfig	Automatic Configuration - Auto-Config Source and Target Node Profiles.
autoconfig.AutoConfigScriptManager.method_configure	Automatic Configuration - method_configure - Ability to create/modify/delete an auto-config script.
autoconfig.AutoConfigScriptManager.method_copyContents	Automatic Configuration - method_copyContents - Ability to copy the contents of one auto-config script to new one.
bfd	BFD - Bi-Directional Forwarding Detection (BFD) can be configured on rtr.NetworkInterface, ies.L3AccessInterface, vprn.L3AccessInterface and vprn.NetworkInterface.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
bgp	Routing Management: BGP - Border Gateway Protocol (BGP) configuration for routers, policies, peers, groups, MD5, and Confederations.
bgp.Site	BGP Site - Access to a BGP protocol site on a router.
bulk	Bulk Operations - Not currently used.
bulk.BulkChange	Bulk Change - The ability to create, modify, and/or delete bulk changes.
bulk.BulkManager.method_execute	Bulk Operations Manager - method_execute - The ability to execute bulk operations.
bulk.BulkManager.method_generateBatches	Bulk Operations Manager - method_generateBatches - The ability to generate batches for bulk operations.
bundle	Bundle - Bundle configuration for T1/E1 Multilink Group and channel members, APS, Multichassis and Service interfaces.
cac	CAC - CAC configuration for Physical Links, Physical Port and other CAC related objects.
ccag	CCAG - Cross-Connect Aggregation Group (CCAG) MDA card and forwarding path configuration.
cflowd	Cflowd - CFLOWD Objects.
cflowd.NeCflowd	Cflowd Configuration - Ability to configure cflowd params for SR.
cflowd.NeCollector	Cflowd Collector Configuration - Ability to configure collector for cflowd params for SR.
clear	Clear - Clear application commands and requests.
cli	CLI - Ability to connect to open NE sessions from the NFM-P.
cli.SSH	SSH Session - Ability to open an SSH Telnet session to the node from the NFM-P.
cli.Telnet	Telnet Session - Ability to open a Telnet session to the node from the NFM-P.
connprof	Connection Profile - Connection Profile configuration.
cpipe	CPipe - Access to this package is for configuring CES Interface Specifics for Cpipe specific SAPs.
cpipe.Cpipe	Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
cpipe.Site	Cpipe Site - Access to Cpipe Sites.
crdtctrl	Credit Control - Credit Control configuration.
customproperties	Custom Properties - Custom properties configuration.
db	Database - Configuration for Size constraint policies and Database file policies.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
db.DatabaseManager.method_backup	Database Manager - method_backup - Ability to perform a database backup.
db.DatabaseManager.method_reinstantiateStandby	Database Manager - method_reinstantiateStandby - Ability to reinstantiate the standby database.
db.DatabaseManager.method_switchover	Database Manager - method_switchover - Ability to perform a database switchover.
dctr	Data Center - Data Center information and configurations.
dctr.PortProfile	Port Profile - Configuration of Port Profile.
dctr.VirtualSpokeSdpBinding	Virtual Spoke SDP Binding - Access to Virtual Spoke SDP Binding configuration.
dctr.VlanRange	VLAN Range - Configuration of Vlan Entry.
dctr.VplsVirtualSite	Virtual Site VPLS - Access to VPLS eVPN-Sites on a VPLS Service.
dctr.VprnVirtualSite	Virtual Site VPRN - Access to VPLS eVPN-Sites on a VPLS Service.
dhcp	DHCP - Dynamic Host Configuration Protocol (DHCP) Server for rtr.VirtualRouter and vprn.Site.
diameter	Diameter - Access to this package is for configuring Diameter related configurations, e.g. Diameter Policy.
dns	Domain Name System - Domain Name System.
dynsvc	Dynamic Services - Dynamic Services Configuration.
entity	Physical Entity Management.
epipe	EPipe - Access to this package is for configuring CES Interface Specifics and FR Interface Specifics for Epipe specific SAPs.
epipe.Epipe	Epipe Service - Access to VLL Ethernet Pipe (Epipe) Service objects themselves.
epipe.PbbMacName	PBB MAC Name - Ability to configure the MAC Name Address for a Network Element.
epipe.Site	Epipe Site - Access to Epipe Sites.
equipment	Physical Equipment - General equipment configuration.
equipment.PortPolicy	Port Policy - Access to Port Policy for 7750 nodes.
equipment.Shelf.method_rebootUpgrade	Shelf - method_rebootUpgrade - Ability to perform node reboot upgrade.
ethernetequipment	Ethernet Equipment - Ethernet Equipment configuration.
ethernetoam	Ethernet OAM - Maintenance Domains and Maintenance Entity Groups, autogeneration of the MEPs on each SAP or Binding in a Service.
ethernetoam.CcmTest	CFM Continuity Check - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
ethernetoam.CcTest	Global Maintenance Entity Group - Access to Continuity Check tests, Continuity Check test definitions, and Continuity Check deployed tests.
ethernetoam.CfmDmmBin	CFM DMM Session Bin - Access to CFM DMM Test Session, CFM DMM Test Session definitions.
ethernetoam.CfmDmmSession	CFM DMM Test Session - Access to CFM DMM Test Session, CFM DMM Test Session definitions.
ethernetoam.CfmEthTest	CFM Eth Test - Access to CFM EthTests, CFM EthTest definitions, and CFM EthTest deployed tests.
ethernetoam.CfmLinkTrace	CFM Link Trace - Access to Link Trace tests, Link Trace test definitions, and Link Trace deployed tests.
ethernetoam.CfmLmmSession	CFM LMM Test Session - Access to CFM LMM Test Session, CFM LMM Test Session definitions.
ethernetoam.CfmLMTest	CFM LM Test - Access to CFM LM tests, CFM LM test definitions, and CFM LM deployed tests.
ethernetoam.CfmLoopback	CFM Loopback - Access to CFM Loopback tests, CFM Loopback test definitions, and CFM Loopback deployed tests.
ethernetoam.CfmOneWayDelayTest	CFM One Way Delay Test - Access to CFM One Way Delay tests, CFM One Way Delay test definitions, and CFM One Way Delay deployed tests.
ethernetoam.CfmOneWaySlm	CFM One Way SLM Test - Access to CFM One Way SLM tests, CFM One Way SLM test definitions, and CFM One Way SLM deployed tests.
ethernetoam.CfmSingleEndedLossTest	CFM Single Ended Loss Test - Access to CFM Single Ended Loss tests, CFM Single Ended Loss test definitions, and CFM Single Ended Loss deployed tests.
ethernetoam.CfmSlmSession	CFM SLM Test Session - Access to CFM SLM Test Session, CFM SLM Test Session definitions.
ethernetoam.CfmTwoWayDelayTest	CFM Two Way Delay Test - Access to CFM Two Way Delay tests, CFM Two Way Delay test definitions, and CFM Two Way Delay deployed tests.
ethernetoam.CfmTwoWaySlm	CFM Two Way SLM Test - Access to CFM Two Way SLM tests, CFM Two Way SLM test definitions, and CFM Two Way SLM deployed tests.
ethernetoam.EthSession	Ethernet Test Session - Access to Ethernet Test Session, Ethernet Test Session definitions.
ethernetservice	Ethernet Service Policy - SAP Profile and UNI Profile policies.
ethernettunnel	Ethernet Tunnel - Ethernet Tunnel configuration.
ethring	Ethernet Ring - Ethernet Ring Configuration.
event	events - Parent package for all event classes.
fabricqos	Fabric QoS Policies - Fabric Profile QoS policy.
file	File Policy - File creation on the NE for events and accounting.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
filter	Filter - Public search filters.
filterprefixlist	Filter Policy - Filter PrefixList and PortList Policies.
firewall	Firewall - All Firewall configurations.
fm	Fault Management - Alarm policies, Severity change thresholds, Alarms, Notes, and History.
fm.AlarmHistoryDatabase.method_purge	Alarm History Database - method_purge - Ability to purge the alarm history database.
fm.FaultManager	Fault Manager - Access to assign OLC state, alter severity, clear, acknowledge, and remove faults.
fm.FaultManager.method_editNote	Fault Manager - method_editNote - Ability to edit an alarm note.
fm.GlobalPolicy	Global Alarm Behavior - Access to configure the global alarm behavior.
fm.SpecificPolicy	Specific Alarm Policy - Access to configure specific alarm policies.
fpipe	FPipe - All contained objects are listed. Package access is not currently used.
fpipe.Fpipe	Fpipe Service - Access to Frame Relay Pipe (Fpipe) Service objects themselves.
fpipe.Site	Fpipe Site - Access to Fpipe Sites.
fr	Frame Relay - Frame Relay configuration for Service interfaces and routers.
generic	Generic - Generic configuration for NFM-P objects, deployment, and administrative state changes for DHCP and Multichassis objects, Maintenance Association End Points (MEP), and SRRP instances.
generic.GenericObject.method_collectData	Generic Object - method_collectData - Ability to collect and plot real-time statistics.
genericlog	Log Viewer - Display logs in Log Viewer.
genericne	Generic NE - Generic NE Interface and Profile configuration.
genericne.GenericNeProfileManager.method_ checkFileContent	Generic NE Profiles - method_checkFileContent - Checks the descriptor installation package content for validity.
genericne.GenericNeProfileManager.method_installFile	Generic NE Profiles - method_installFile - Ability to install a descriptor driver.
gmpls	ASON Domain Management - GMPLS Management.
gmplsuni	GMPLS-UNI - GMPLS-UNI Configuration.
gsmp	GSMP - General Switch Management Protocol (GSMP) configuration for VPLS, MVPLS and VPRN routing instances.
histcorr	Historical Correlation - Historical Correlation configuration.
hpipe	HPipe - All contained objects are listed. Package access is not currently used.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
hpipe.Hpipe	Hpipe Service - Access to HPipe (Hpipe) Service objects themselves.
hpipe.Site	Hpipe Site - Access to Hpipe Sites.
icmp	ICMP - Internet Control Message Protocol (ICMP) and Domain Name System (DNS) test results.
icmp.DnsPing	DNS Ping - Access to DNS Ping tests, DNS Ping test definitions, and DNS Ping deployed tests.
icmp.IcmpPing	ICMP Ping - Access to ICMP Ping tests, ICMP Ping test definitions, and ICMP Ping deployed tests.
icmp.IcmpTrace	ICMP Trace - Access to ICMP Trace tests, ICMP Trace test definitions, and ICMP Trace deployed tests.
ies	IES - Access to this package is for configuring Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for IES specific SAPs.
ies.Ies	IES Service - Access to Internet Enhanced Service (IES) Service objects themselves.
ies.L3AccessInterface	IES L3 Access Interface - Access to IES L3 Access Interfaces.
ies.Site	IES Site - Access to IES Sites.
ies.SubscriberInterface	IES Subscriber Interface - Access to IES Subscriber Interfaces.
igh	IGH - Interface-Group-Handlers.
igmp	IGMP - Internet Group Management Protocol (IGMP) configuration for Service interfaces and routers.
igmp.Site	IGMP Site - Access to IGMP Sites.
impact.FullReset	Full Reset - Ability to configure objects which will result in a full reset of the node. Currently applies to 9412 node.
impact.PartialReset	Partial Reset - Ability to configure objects which will result in a partial reset of impacted SW/HW unit. Currently applies to 9412 node.
ipdr	IPDR File Transfer Policies - IPDR file transfer policies.
ipfix	IPFIX - IPFIX Policy.
ipipe	IPipe - Access to this package is for configuring IPCP on L2 Access Interfaces and FR Interface Specifics for Ipipe specific SAPs.
ipipe.Ipipe	Ipipe Service - Access to IP Interworking Pipe (Ipipe) Service objects themselves.
ipipe.L2AccessInterface	L2 Access Interface - Access to IPipe L2 Access Interfaces.
ipipe.Site	Ipipe Site - Access to Ipipe Sites.
ipsec	IP Security - IKE Policy and IPsec Transform.
isa	ISA - ISA-IPsec, ISA-MG configuration on a MDA card for IP Security.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
isa.IPSecMgIsaGroup	ISA IPSMG Group - Configuration of IPSec ISA-MG Group.
isa.IPSecMgIsaGroupMdaAssociation	ISA-IPSMG Group MDA Association - Configuration of ISA-IPSMG Group MDA Association.
isa.MgGroupMember	ISA-MG Group Member - Configuration of ISA-MG Group Member.
isa.MgIsaGroup	ISA-MG Group - Configuration of ISA-MG Group.
isis	Routing Management: ISIS - IS-IS configuration for Service interfaces and routers, Area, Adjacency, Neighbors, Policies and other IS-IS related objects.
l2fib	L2 FIB - Layer 2 Forwarding Information Base (FIB) configuration for Multicast and Non-Multicast.
l2fwd	L2 Forwarding - All Layer 2 Forwarding configuration for Service interfaces and routers, circuits, ports, Spanning Tree, Registration, FIB, Mac Protection, IGMP Snooping, etc.
l2tp	L2TP - L2TP configuration for Service interfaces and routers, Groups, Tunnels, PeersRPs, and other L2TP related objects.
l3fwd	L3 Forwarding - All Layer 3 Forwarding configuration for Service interfaces and routers, Import and Export policies, Dot1p and DSCP for VPRNs.
lag	LAG - Link Aggregation Group (LAG) configuration for Service interfaces and routers.
layer2	Layer 2 - All Layer 2 configuration: Bridges, Transparent LAN Service (TLS), and VLAN interfaces.
ldp	Routing Management: LDP - Label Distribution Protocol (LDP) configuration for Service interfaces and routers, Session, MD5 Key, Equal-Cost Multipath Routing (EMCP), Forwarding Equivalency Class (FEC), Policies, and Peers.
lldp	LLDP - Link Layer Discovery Protocol (LLDP) configuration on equipment.PhysicalPort.
lmg	LMG - All LMG configurations and status.
lmgperf	LMG Performance Management - All LMG configurations.
lmp	LMP - LMP Configuration for Sites.
localuserdb	Local User DB - DHCP or PPPoE configuration for Local User Databases on a router.
log	Statistics - Parent package for all statistics classes.
log.LogToFileManager.property_jmsRetries	Log To File Manager - property_jmsRetries - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_retention	Log To File Manager - property_retention - LogToFile preferences can only be modified by a user with an administrator role.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
log.LogToFileManager.property_rollover	Log To File Manager - property_rollover - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_storeAccountingStatsInDB	Log To File Manager - property_storeAccountingStatsInDB - LogToFile preferences can only be modified by a user with an administrator role.
log.LogToFileManager.property_ storePerformanceStatsInDB	Log To File Manager - property_storePerformanceStatsInDB - LogToFile preferences can only be modified by a user with an administrator role.
lps	LPS - Learned Port Security (LPS) configuration for layer2.Bridge and MAC Entries for ports.
mediation	Router Admin: Policies - Router administration: Backup Policies, Upgrade Policies and Software images, Deployment Policies, and Management Ping Policies.
mirror	Mirror - All configurations for Service Mirroring.
mirror.Endpoint	Endpoint - Access to MIRROR Endpoints.
mirror.Mirror	Mirror Service - Access to Mirror Service objects themselves.
mirror.Site	Mirror Site - Access to Mirror Sites.
mld	MLD - Multicast Listener Discovery Protocol (MLD) configuration for a Service interfaces and routers.
monitor	Monitor - Subscriber Host monitoring and SAP monitoring.
monpath	Monitored Path - IP path monitoring and LSP monitoring.
mpls	Path/Routing Management: MPLS - Multiprotocol Label Switching (MPLS) configuration on a rtr.VirtualRouter, LSPs, Segments, Hops, Tunnels, CrossConnects, and other MPLS related objects.
mpls.LdpTreeTrace	LDP Tree Trace - Access to LDP Tree Trace tests, LDP Tree Trace test definitions, and LDP Tree Trace deployed tests.
mpls.LspPing	LSP Ping - Access to LSP Ping tests, LSP Ping test definitions, and LSP Ping deployed tests.
mpls.LspTrace	LSP Trace - Access to LSP Trace tests, LSP Trace test definitions, and LSP Trace deployed tests.
mpls.P2MPLspPing	P2MP LSP Ping - Access to P2MP LSP Ping tests, P2MP LSP Ping test definitions, and P2MP LSP Ping deployed tests.
mpls.P2MPLspTrace	P2MP LSP Trace - Access to P2MP LSP Trace tests, P2MP LSP Trace test definitions, and P2MP LSP Trace deployed tests.
mplstp	MPLS TP - MPLS TP Configuration for Sites.
mpr	9500 MPR - 9500 Microwave Packet Radio (MPR) VLAN Paths and Hops.
mpr.Cpipe	9500 MPR Cpipe Service - Access to VLL Circuit Emulation Pipe (Cpipe) Service objects themselves.
mpr.El2AccessInterface	9500 MPR Epipe L2 Access Interface - Access to L2AccessInterface objects.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
mpr.Epipe	9500 MPR Epipe Service - Access to VLL Ethernet Pipe Service objects themselves.
mpr.Esite	9500 MPR Epipe Site - Access to the service instance objects.
mpr.L2AccessInterface	9500 MPR Cpipe L2 Access Interface - Access to L2AccessInterface objects.
mpr.Site	9500 MPR Cpipe Site - Access to the service instance objects.
msappolicy	MSAP Policy - MSAP policy configuration.
msdp	MSDP - Multicast Source Discovery Protocol (MSDP) configuration for a rtr.VirtualRouter, MD5 Key, Peers, Policies and Source.
multicast	Multicast - Multicast Connection Admission Control (CAC) Policies and Bandwidth Policies.
multicast.CustomerVlanTag	Customer Vlan Tag - Configuration of Customer VLAN Tags for a Multicast VLAN.
multicast.MfibPing	MFIB Ping - Access to MFIB Ping tests, MFIB Ping test definitions, and MFIB Ping deployed tests.
multicast.Mrinfo	Mrinfo - Access to Mrinfo tests, Mrinfo test definitions, and Mrinfo deployed tests.
multicast.Mtrace	Mtrace - Access to Mtrace tests, Mtrace test definitions, and Mtrace deployed tests.
multicastmgr	CPAM: Multicast - All CPAM Multicast related objects: PIM Domain, VPLS Domain, Groups, and Sources.
multichassis	Multi-Chassis - Multi-Chassis configuration for a router; LAGs, Rings, Syncs, Peers, VLAN Ranges, IPsecs.
mvpls	MVPLS - All contained objects are listed. Package access is not currently used.
mvpls.BL2AccessInterface	MVPLS B-L2 Access Interface - Access to MVPLS B-L2 Access Interfaces.
mvpls.BSite	MVPLS B-Site - Access to MVPLS B-Sites.
mvpls.EvpnSite	MVPLS EVPN-Site - Access to MVPLS EVPN-Sites on a MVPLS Service.
mvpls.IL2AccessInterface	MVPLS I-L2 Access Interface - Access to MVPLS I-L2 Access Interfaces.
mvpls.ISite	MVPLS I-Site - Access to MVPLS I-Sites.
mvpls.L2AccessInterface	MVPLS L2 Access Interface - Access to MVPLS L2 Access Interfaces (except I and B).
mvpls.Mvpls	MVPLS Service - Access to Management Virtual Private LAN Service (MVPLS) Service objects themselves.
mvpls.Site	MVPLS Site - Access to MVPLS Sites (except I and B).
mvrp	MVRP - MVRP global configuration and for Interfaces(Ports and LAG's).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
mwa	Microwave Aware - Access to MW (Microwave) Link and MW Link Members configuration for Service interfaces and routers.
nat	Network Address Translation - NAT Policy.
nat.LsnSubSession	LSN Subscriber Session - Access to NAT Package.
nat.PcpServer	Port Control Protocol Server - Access to Port Control Protocol Server configuration.
nat.PcpServerInterface	Port Control Protocol Server Interface - Access to Port Control Protocol Interface configuration.
neaudit	NE Audit Management - Ability to manage NE Audits.
negcss	Network Element Golden Config Snapshot - Golden Config Webapp.
nelicense	NeLicense - Apply License on the node.
netca	NE Threshold Crossing Alerts - Manage NE Threshold Crossing Alert profiles.
netw	Network - Network objects: groups and links.
netw.AdvertisedNode	Advertised Node - Control of Discovered Nodes.
netw.NeLimitHolder	NE Limits - Access to NE Limit configuration.
netw.NetworkElement	Network Element - Access to Network Elements.
netw.NetworkElement.method_executeCli	Network Element - method_executeCli - Execute a single raw CLI command on this Network Element.
netw.NetworkElement.method_executeMultiCli	Network Element - method_executeMultiCli - Execute Multiple CLI commands on this Network Element.
netw.NetworkElement.method_GUICrossLaunch	Network Element - method_GUICrossLaunch - The ability to launch LTE web-browser based tools.
netw.NetworkElement.method_ NetoAdminProfileBasedLaunch	Network Element - method_NetoAdminProfileBasedLaunch - The ability to launch Neto with Admin profile.
netw.NetworkElement.method_ NetoViewerProfileBasedLaunch	Network Element - method_NetoViewerProfileBasedLaunch - The ability to launch Neto with Viewer profile.
netw.NetworkElement.property_elementManagerCmd	Network Element - property_elementManagerCmd - Ability to update the 'Alternate Element Manager' command for a GNE.
netw.NodeDiscoveryControl	Node Discovery Control - Control of Discovered Nodes.
netw.Topology	Discovery Manager - Access to the Discovery Manager.
netw.Topology.method_move	Discovery Manager - method_move - Ability to move a node or group on the NFM-P Client GUI maps.
netw.UplinkBofConfiguration	Uplink Bof Configuration - Ability to configure the Uplink BOF for a 7210 node.
netw.UplinkRouteConfiguration	Uplink Route Configuration - Ability to configure the Uplink Routes for a 7210 node.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
nge	NetworkGroupEncryption - Network Group Encryption configuration on 7705 router.
niegr	Network Ingress/Egress Policy - Network Policies.
nodelog	Node Log Policy - Filter Log and Sys Log Target Policies.
nqueue	Network Queue Policy - Network Queue QoS Policies.
ntp	Network Time Protocol - Network Time Protocol.
ntp.NTPBroadcast	NTP Broadcast - Ability to configure broadcast for ntp params.
ntp.NTPMulticast	NTP Multicast - Ability to configure multicast for ntp params.
olc	Object Life Cycle.
olc.OLCSchedulerManager.property_ autosetMaintenanceOLCStateOnAdminDown	OLC Scheduler Manager - property_ autosetMaintenanceOLCStateOnAdminDown - Service preferences can only be modified by a user with an administrator role.
olc.OLCSchedulerManager.property_ createAlarmNotification	OLC Scheduler Manager - property_createAlarmNotification - OLC preferences can only be modified by a user with an administrator role.
olc.OLCSchedulerManager.property_ leadTimeForNotification	OLC Scheduler Manager - property_leadTimeForNotification - OLC preferences can only be modified by a user with an administrator role.
openflow	OpenFlow - OpenFlow configuration and status on a router.
optical	Optical Management - Optical NE Specific Information.
optical.MultipointServicePath	Multipoint Service Path - Access for all Multi Point Service Paths.
optical.MultipointTransportService	Multipoint Transport Service - Access for all optical services.
optical.OCHTrail	OCH Trail - Access for all OCH trails.
optical.ODUTrail	ODU Trail - Access for all ODU trails.
optical.OMSTrail	OMS Trail - Access for all OMS trails.
optical.OTSTrail	OTS Trail - Access for all OTS trails.
optical.OTUTrail	OTU Trail - Access for all OTU trails.
optical.STMTrail	STM Trail - Access for all STM trails.
optical.TransportService	Optical Transport Service - Access for all optical services.
opticalacl	Optical Access Control Lists - ACL Management.
opticalequipment	Optical Management - Optical NE Specific Configuration.
opticalrouting	Optical Routing - Optical Routing Meta.
opticsperf	Optics Specifics - All 1830 PSS configurations.
ospf	Routing Management: OSPF - OSPF configuration for Service interfaces and routers, Area, Adjacency, MD5 Key, Virtual Links Neighbors, LSAs, Policies and other OSPF related objects.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
ospf.Site	OSPF Site - Access to OSPF Sites.
oss	XML API - Ability to connect to the NFM-P through the XML API interface.
oth	Optical Transport Hierarchy - OTH Management.
pae802_1x	PAE 802.1x - Port Access Entity (PAE) configuration for a router and physical port; RADIUS Server Policy.
pbbvlan	PBBVLAN - Access to this package is for configuring SPB-BVLAN Service, Site, SAPs, MeshSDPs and site statistics.
pbbvlan.Site	SPB Site - Access to SPB Services.
pbbvlan.VlanPBBEdge	SPB Service - Access to SPB Services.
pim	PIM - PIM configuration for Service interfaces and routers, MDT Threshold, Policies, Neighbors, Groups, RPs, Multicast CAC Level and LAG Port Down events, and other PIM related objects.
pim.Site	PIM Site - Access to PIM Sites.
policing	Policing Policy - Policer Control.
policy	Policy - Parent package for all policies; Policy Audits, Policy Export/Imports.
policy.PolicyDefinition.method_ setConfigurationModeToReleased	Policy Definition - method_setConfigurationModeToReleased - Ability set Configuration Mode to Released and distribute the global policy to the local definitions network-wide.
policy.PolicyDefinition.method_ setDistributionModeToLocalEditOnly	Policy Definition - method_setDistributionModeToLocalEditOnly - Ability set Configuration Mode to Local Edit Only for local policies and ignore changes to the global policy.
policy.PolicyDefinition.method_ setDistributionModeToSyncWithGlobal	Policy Definition - method_setDistributionModeToSyncWithGlobal - Ability set Configuration Mode to Sync with Global and synchronize local policies with the most recent released global policy.
policy.PolicyNameManager.property_ autoDistributeOnRelease	Policies - property_autoDistributeOnRelease - Policy preferences can only be modified by a user with an administrator role.
policy.PolicyNameManager.property_localEditOnly	Policies - property_localEditOnly - Policy preferences can only be modified by a user with an administrator role.
policy.PolicyNameManager.property_ localEditOnlyOnCLIChange	Policies - property_localEditOnlyOnCLIChange - Policy preferences can only be modified by a user with an administrator role.
policy.PolicyNameManager.property_ maxScheduledAuditResultPerLocalPolicy	Policies - property_maxScheduledAuditResultPerLocalPolicy - Policy preferences can only be modified by a user with an administrator role.
policy.PolicyNameManager.property_ securityZoneDiscoveredInLocalEditOnlyMode	Policies - property_securityZoneDiscoveredInLocalEditOnlyMode - Policy preferences can only be modified by a user with an administrator role.
policy.PolicyNameManager.property_ showFilterDisplayName	Policies - property_showFilterDisplayName - Policy preferences can only be modified by a user with an administrator role.
policy.PolicyNameManager.property_ showQoSPolicyDisplayName	Policies - property_showQoSPolicyDisplayName - Policy preferences can only be modified by a user with an administrator role.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
policy.PolicySyncGroupManager	Policy Sync Group - Ability to configure and control policy sync group.
policy.ProfileManager	Profile Manager - Ability to configure and control profiles.
policytestutil	Policy Test Utility - TODO.
port.RestrictModeConfigModify	port.RestrictModeConfigModify - Ability to restrict Port Mode modification for Ports with dependencies.
portscheduler	Port Scheduler Policy - Port Scheduler and HSMDA Scheduler Policies.
ppp	PPP - Point-to-Point Protocol (PPP) configuration on a router.
pppoe	PPP Policy and Session - Point-to-Point Protocol over Ethernet over ATM (PPPoE/PPPoEoA/PPPoA) Policies and Sessions.
propertyrules	Property Rules - Range and Format Value Policies.
ptp	Precision Timing Protocol - Access to this package is for configuring Precision Timing Protocol.
pxc	PXC - Port Cross Connect.
qgroup	Queue Group Policy - Queue Group Policies.
qosprefixlist	QoS Policy - QoS PrefixList Policy.
qosprofile	Multilink QoS Profile - Multilink PPP QoS Profiles and Multilink Frame Relay QoS Profiles.
radioequipment	Radio Equipment - Radio Equipment configuration.
radiusaccounting	Radius Accounting - Radius Accounting Policy.
ranlicense	NE License Management - Ability to manage NE licenses.
rca	RCA - Root Cause Analysis (RCA) for verification functions (OSPF Area, IS-IS Area, BGP AS, ..).
rca.RcaManager.method_fixProblem	Rca Manager - method_fixProblem - Ability to fix a problem on an object.
rca.RcaManager.method_preFixProblem	Rca Manager - method_preFixProblem - Ability to determine if a problem can be fixed, and the fix impact.
redirectfilter	Redirect Filter Policy - Redirect Filters.
resiliency	HSDPA Resiliency - HSDPA Resiliency for services.
resources	NFM-P Resources - NFM-P Resource Pools as configured in the nms-server.xml file.
ressubscr	Residential Subscriber - All Residential Subscriber configuration including Connectivity Verifications (SHCV), SAPs, Packages, Hosts, QoS, and other related objects.
ressubscr.BgpPeeringPolicy	BGP Peering Policy - Access to BGP Peering Policies.
ressubscr.HostTrackingPolicy	Host Tracking Policy - Access to Host Tracking Policies.
ressubscr.IgmpPolicy	IGMP Policy - Access to IGMP Policies.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
ressubscr.IpoePolicy	IPoE Session Policy - Access to IPoE Session Policies.
ressubscr.MldPolicy	MLD Policy - Access to MLD Policies.
ressubscr.ResidentialSubscriberManager.property_hostTrkSubscrRtrvTimeOut	Residential Subscriber Manager - property_hostTrkSubscrRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_qbtUeRtrvTimeOut	Residential Subscriber Manager - property_qbtUeRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_resSubscrInstRtrvMax	Residential Subscriber Manager - property_resSubscrInstRtrvMax - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveAcclpEncap	Residential Subscriber Manager - property_retrieveAcclpEncap - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveBgpPeerInfo	Residential Subscriber Manager - property_retrieveBgpPeerInfo - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveBgpPeerV6Info	Residential Subscriber Manager - property_retrieveBgpPeerV6Info - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveManagedRoutes	Residential Subscriber Manager - property_retrieveManagedRoutes - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveQoSOvr	Residential Subscriber Manager - property_retrieveQoSOvr - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_retrieveSlaacHostAddr	Residential Subscriber Manager - property_retrieveSlaacHostAddr - Service preferences can only be modified by a user with an administrator role.
ressubscr.ResidentialSubscriberManager.property_subscriberHostRtrvTimeOut	Residential Subscriber Manager - property_subscriberHostRtrvTimeOut - Service preferences can only be modified by a user with an administrator role.
ressubscr.ShcvPolicy	SHCV Policy - Access to SHCV Policies.
ressubscr.SubMcastCacPolicy	Subscriber Multicast CAC Policy - Access to Subscriber Multicast CAC Policies.
rip	Routing Management: RIP - Routing Information Protocol (RIP) configuration for Service interfaces and routers, Authentication Key, Groups, Export and Import Policies.
rip.Site	RIP Site - Access to RIP Sites.
rmd	Remote Managed Device - Remote Managed Device Management.
rmon	Remote Network Monitoring - Remote Network Monitoring Alarm and Event Policies.
rollback	Rollback - All scheduled tasks; Cron Actions, XML API Commands, CLI Scripts and Schedules.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
rp	Routing Policy - Policy Statements, Prefix Lists, Communities, Damping, and AS Paths.
rsvp	Routing Management: RSVP - RSVP configuration for a rtr.VirtualRouter, Authentication Keys, and Neighbors.
rtr	Routing Management: General - General rtr.VirtualRouter configurations including Neighbor Discovery, DHCP Relays, Interfaces, Peers, Address Ranges and ARP, Routes and Router Advertisement.
rules	Rules - Rule Repository and Sets of rules that may get invoked when a rule engine is fired.
sas	Assurance - Parent package for all tests; Service Test Manager.
sas.IPSession	IP Session - Access to IP Session, IP Test Session definitions.
sas.TestManager.property_contextNonSapMax	Service Test Manager - property_contextNonSapMax - OAM Context preferences can only be modified by a user with an administrator role.
sas.TestManager.property_contextSapMax	Service Test Manager - property_contextSapMax - OAM Context preferences can only be modified by a user with an administrator role.
sas.TestManager.property_defaultTestResultStorage	Service Test Manager - property_defaultTestResultStorage - These preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasNumberOfHours	Service Test Manager - property_sasNumberOfHours - These preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRetention	Service Test Manager - property_sasRetention - LogToFile preferences can only be modified by a user with an administrator role.
sas.TestManager.property_sasRollover	Service Test Manager - property_sasRollover - LogToFile preferences can only be modified by a user with an administrator role.
sas.TWLBin	TWAMP Light Session Bin - Access to TWAMP Light Test Session, TWAMP Light Test Session definitions.
sas.TwlReflector	TWAMP Light Reflector - Access to TWAMP Light Reflector.
sas.TWLSession	TWAMP Light Test Session - Access to TWAMP Light Test Session, TWAMP Light Test Session definitions.
sas.VxlanPing	VXLAN Ping - Access to VXLAN Ping tests, VXLAN Ping test definitions, and VXLAN Ping deployed tests.
saspm	SAS PM - Access to OAM Performance Monitoring Objects.
sasqos	7210 and 1830 QoS - QoS Policies for 7210 and 1830 nodes.
sasqos.QosPool	QoS Pool - Access to QoS Pools for 7210 nodes.
schedule	Schedule - All scheduled tasks; Cron Actions, XML API Commands, CLI Scripts and Schedules.
script	Scripting - Script Management and execution of Service and Tunnel Template, XML API, and CLI scripts.
script.AbstractScript.method_configureTarget	Script - method_configureTarget - Ability to configure targets and instances.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
script.AbstractScript.method_configureTargets	Script - method_configureTargets - Ability to configure targets and instances.
script.Bundle	Script Bundle - Ability to configure script bundles.
script.ControlScript	Control Script - Ability to configure control scripts.
script.ControlScriptVersion	Control Script Version - Ability to configure Control script versions.
script.HandlerBinding	Handler Script Binding - Ability to configure associations between scripts and control scripts.
script.InvokerBinding	Invoker Script Binding - Ability to configure associations between scripts and control scripts.
script.JsonTargetParameter	JSON Target Parameter - Ability to configure target/instance JSON parameters.
script.LargeTextTargetParameter	Large Text Target Parameter - Ability to configure target/instance large text parameters.
script.Result	Result - Ability to create script results.
script.Script	CLI Script - Ability to configure CLI scripts.
script.Script.method_createTargetScript	CLI Script - method_createTargetScript - Ability to configure targets.
script.Script.method_createTargetScripts	CLI Script - method_createTargetScripts - Ability to configure targets.
script.ScriptManager	Script Manager - Ability to configure and control scripts and script operations.
script.ScriptManager.method_configure	Script Manager - method_configure - Ability to configure scripts.
script.ScriptManager.method_copyContents	Script Manager - method_copyContents - Ability to copy scripts.
script.ScriptManager.method_exportBundle	Script Manager - method_exportBundle - Ability to export bundle.
script.ScriptManager.method_importBundle	Script Manager - method_importBundle - Ability to import bundle.
script.ScriptManager.method_importBundleSimulation	Script Manager - method_importBundleSimulation - Ability to import bundle.
script.ScriptScheduledTask	Script Scheduled Task - Ability to schedule a script.
script.TargetParameter	Target Parameter - Ability to configure target/instance parameters.
script.TargetParameterItem	Target Parameter Item - Ability to configure target/instance parameter items.
script.TargetParameterList	Target Parameter List - Ability to configure target/instance parameter lists.
script.TargetScript	Target Script - Ability to configure targets and instances.
script.TemplateBinding	Template Binding - Ability to configure associations between templates.
script.Version	Version - Ability to configure CLI script versions.
script.XmlApiConfigTemplate	Template - Ability to configure XML API templates.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
script.XmlApiConfigTemplate.method_execute	Template - method_execute - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeMulti	Template - method_executeMulti - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_executeScript	Template - method_executeScript - Ability to create an object from a template.
script.XmlApiConfigTemplate.method_ serviceTemplateExecute	Template - method_serviceTemplateExecute - Ability to execute a service template.
script.XmlApiConfigTemplate.method_ tunnelTemplateExecute	Template - method_tunnelTemplateExecute - Ability to execute a tunnel template.
script.XmlApiScript	XMLAPI Script - Ability to configure XML API scripts.
script.XmlApiVersion	XMLAPI Version - Ability to configure XML API script versions.
security	Security - NFM-P User security including Sessions, TCP KeyChains, and SSH2 Known Host Keys.
security.MediationPolicy	Mediation Policy - Access to Mediation Policies. Used in conjunction with snmp.PollerManager.
security.MessagingConnection	Messaging Connection - Ability to view messaging connections.
security.RoleBasedAccess	security.RoleBasedAccess - Ability to restrict online object creation and deletion to a specific role. Currently applies to 9412 node.
security.ScopeOfCommandProfile	Profile - Access to Scope of Command Profile configuration.
security.ScopeOfCommandRole	Role - Access to Scope of Command Role configuration.
security.Span	Span - Access to Span configuration. Used in conjunction with security.SpanObjectBinding.
security.SpanObjectBinding	Span Objects - Access to Span object configuration. Used in conjunction with security.Span.
security.SpanOfControlProfile	Profile - Access to Span of Control Profile configuration.
security.User	User - Access to User object configuration and password changes.
security.UserGroup	User Group - Access to UserGroup configuration.
securitypolicy	Security Policy - All Security configurations including security policy,profile,zone,NAT.
securityqueue	Security Queue QoS Policies - Security Queue QoS policy.
selfconfig	Self Config - Ability to configure self config objects.
server	NFM-P Server - NFM-P Servers (JMS, Main, Auxilary Server, Auxiliary Database) as configured in the nms-server.xml file.
service	Service Management - Parent package for all services; Composite Services and Connectors and Access Policy Queue Override Policies.
service.AarpInterface	AARP Interface - Access to AARP Interface configuration between AARP.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
service.CpePing	CPE Ping - Access to CPE Ping tests, CPE Ping test definitions, and CPE Ping deployed tests.
service.GneAccessInterface	GNE Service Interface - Access to GNE Service Interfaces.
service.GneSite	GNE Site - Access to GNE Sites.
service.MacPing	MAC Ping - Access to MAC Ping tests, MAC Ping test definitions, and MAC Ping deployed tests.
service.MacPopulate	MAC Populate - Access to MAC Populate tests, MAC Populate test definitions, and MAC Populate deployed tests.
service.MacPurge	MAC Purge - Access to MAC Purge tests, MAC Purge test definitions, and MAC Purge deployed tests.
service.MacTrace	MAC Trace - Access to MAC Trace tests, MAC Trace test definitions, and MAC Trace deployed tests.
service.RedundantInterface	Redundant Interface - Access to Redundant Interface configuration between SRRP instances.
service.Service.method_create	Service - method_create - Ability to create a service via the NFM-P Client GUI.
service.Service.method_highPriorityServiceDelete	Service - method_highPriorityServiceDelete - Ability to delete high priority Service.
service.Service.property_svcPriority	Service - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceManager.property_ alarmAggregationCompositeService	Service Manager - property_alarmAggregationCompositeService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_alarmAggregationSdp	Service Manager - property_alarmAggregationSdp - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ autoDiscoverCompositeSvc	Service Manager - property_autoDiscoverCompositeSvc - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_enableCac	Service Manager - property_enableCac - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_enableRTConnection	Service Manager - property_enableRTConnection - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ generateReservedRrcAlarm	Service Manager - property_generateReservedRrcAlarm - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ maxNumberOfMoveSites	Service Manager - property_maxNumberOfMoveSites - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ multiSegmentTunnelSelection	Service Manager - property_multiSegmentTunnelSelection - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ propagateServiceNameToSites	Service Manager - property_propagateServiceNameToSites - Service preferences can only be modified by a user with an administrator role.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
service.ServiceManager.property_ propagateSiteNameToService	Service Manager - property_propagateSiteNameToService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ propagateSvcNameDesc	Service Manager - property_propagateSvcNameDesc - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_removeEmptyService	Service Manager - property_removeEmptyService - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_safeSvcDelete	Service Manager - property_safeSvcDelete - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_ supVprnSnmpCommunityStringMsg	Service Manager - property_supVprnSnmpCommunityStringMsg - Service preferences can only be modified by a user with an administrator role.
service.ServiceManager.property_svcPriority	Service Manager - property_svcPriority - Service priority can only be modified by a user with an administrator role.
service.ServiceMemberAuditPolicyEntry	Service Membership Audit Policy Entry - Access to Service Member Audit Policy Entry to configure service membership RCA audit behavior.
service.SitePing	Service Site Ping - Access to Service Site Ping tests, Service Site Ping test definitions, and Service Site Ping deployed tests.
service.TemplateService.method_ constructServiceTemplate	Service Template - method_constructServiceTemplate - Ability to construct a Template from a Service.
service.TemplateService.method_ constructTemplatedService	Service Template - method_constructTemplatedService - Ability to construct a Service from a Template.
service.Y1564TestHeadBiDirectional	Y1564 Bi-Directional Test - Access to Y1564 Bi-Directional tests, Y1564 Bi-Directional test definitions, and Y1564 Bi-Directional deployed tests.
sflow	sFlow - SFLOW Objects.
shaperqos	Shaper QoS Policies - Shaper QoS policy.
shg	Split Horizon Group - Split Horizon Groups for VPLS services.
simulator	CPAM: Simulator - Parent package for all CPAM simulated objects; Scenarios, Sessions, Change and Action events.
simulator.SimSession	Session - Access to simulation sessions for CPAM Impact Analysis.
sitesec	NE Security - All Network Element security configuration including NE System Security, RADIUS, TACACS+ and AOS Authentication, Site Management Access and CPM Filters, DoS Protection, Password Policy, Users and Profiles.
sitesec.LocalUser	NE User - Access to NE Site User configuration.
sitesec.UserProfile	Site User Profile - Access to NE Site User Profile configuration.
sitesec.UserPublicKey	RSA Key - Public keys(SSHv2) configuration for the system users.
slaprofile	SLA Profile - SLA Profiles for QoS Policies.
slope	Slope Policy - WRED Slope, HSMDA WRED Slope, HSMDA Pool, and Named Buffer Pool Policies.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
slope.QosPool	QoS Pool - Access to QoS Pools for 7450 and 7750 nodes.
snmp	SNMP - SNMP Poller Policies, Event Notification Policies, Statistics Poller Policies.
snmp.EventNotificationPolicy	Event Notification Policy - Access to Event Notification Policies.
snmp.PollerManager	Mediation - Access to Mediation Policies. Used in conjunction with security.MediationPolicy.
snmp.PollerManager.method_resync	Mediation - method_resync - Ability to resync a Network Element. Requires 'update' access on netw.NetworkElement.
sonet	SONET Sync - SONET Synchronization for Shelf and Processor Cards.
sonetequipment	SONET Equipment - SONET Equipment configuration.
spanrules	Span Rules - Span Rules for service creation.
spb	SPB - Access to this package is for configuring SPB site and site statistics.
spb.AccessInterface	Access Interface - Access to SPB Interface of VPLS B-L2 Access Interfaces on a BVPLS Service.
spb.NetworkInterface	Network Interface - Access to SPB Network Interfaces.
spb.SpokeSdpBindingInterface	Spoke SDP Binding Interface - Access to SPB Interface of VPLS Spoke-SDP on a BVPLS Service.
squeue	Shared Queue Policy - Shared Queue Policies.
srmrmtauth	NFM-P Remote Authentication - Remote Authentication for NFM-P configuration of RADIUS, TACACS+, and LDAP authentication servers.
srpythonmgmt	Python Management - Python Management.
srrp	SRRP - Subscriber Routed Redundancy Protocol (SRRP) configuration for IES and VPRN services.
statistics	NFM-P Performance Statistics - NFM-P Performance Statistics (Memory, Alarm Rate, Snmp Traps, and Node Resyncs).
statsplot	Statistics Plotter - Statistics Plotter.
subscr	Subscriber Management - Customers configuration.
subscr.Site	Subscriber Site - Access to Subscriber Sites.
subscrauth	Subscriber Authentication - Subscriber Authentication Policy using RADIUS for DHCP sessions.
subscrexpmap	Subscriber Explicit Map - Subscriber Explict Map Entry.
subscrident	Subscriber Identification - Subscriber Identification Policy.
subscrprofile	Subscriber Profile - Subscriber Profile, SLA Entries, Access Policy Queue Overrides and Scheduler Policy Entry Overrides.
sup	Supervision - NFM-P Supervision (Dashboard).

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
svq	Aggregation Scheduler - Service and Subscriber Aggregation Scheduler, Ingress and Egress Aggregation Scheduler Overrides.
svr	Service Routing - All contained objects are listed. Package access is not currently used.
svt	Service Tunnel Management - All Service Tunnel configurations including Clouds, Service Distribution Path (SDP) Bindings and Pseudo Wires.
svt.BvlanTunnel	SPB BVLAN Tunnel (SDP) - Access to vlan Tunnel (SDP) configuration.
svt.L2TPv3Tunnel	L2TPv3 Tunnel (SDP) - Access to l2tpV3 Tunnel (SDP) configuration.
svt.MeshSdpBinding	Mesh SDP Binding - Access to Mesh SDP Binding configuration.
svt.MirrorSdpBinding	Mirror SDP Binding - Access to Mirror SDP Binding configuration.
svt.MtuPing	MTU Ping - Access to MTU Ping tests, MTU Ping test definitions, and MTU Ping deployed tests.
svt.SpokeSdpBinding	Spoke SDP Binding - Access to Spoke SDP Binding configuration.
svt.Tunnel	Tunnel - Access to Tunnel (or SDP object) configuration.
svt.TunnelPing	Tunnel Ping - Access to Tunnel Ping tests, Tunnel Ping test definitions, and Tunnel Ping deployed tests.
svt.VccvPing	VCCV Ping - Access to VCCV Ping tests, VCCV Ping test definitions, and VCCV Ping deployed tests.
svt.VccvTrace	VCCV Trace - Access to VCCV Trace tests, VCCV Trace test definitions, and VCCV Trace deployed tests.
svt.VlanPBBEdgeMeshSdpBinding	PBB VLAN Mesh SDP Binding - Access to PBB VLAN Mesh SDP Binding configuration.
sw	Router Admin: Software - Router administration: Backup Files, Card Software, Upgrade schedules, and Accounting Statistics Retrieval.
sw.BackupRestoreManager.method_backup	Backup/Restore Status - method_backup - Ability to perform a Network Element backup.
sw.BackupRestoreManager.method_restore	Backup/Restore Status - method_restore - Ability to perform a Network Element restore.
sysact	User Activity - User Activity.
taskmgmt	Task Management - Monitor the tasks being executed in the server.
tca	TCA Policy - Parent package for all TCA classes.
tca.TCAManager.property_maxTCAAlarmLimit	TCAManager - property_maxTCAAlarmLimit - TCA preferences can only be modified by a user with an administrator role.
tca.TCAManager.property_maxTCAAlarmResetInterval	TCAManager - property_maxTCAAlarmResetInterval - TCA preferences can only be modified by a user with an administrator role.
tdm	Optical Transport Hierarchy - TDM Management.
tdmequipment	TDM Equipment - TDM Equipment configuration.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
template	Service Template - Deprecated 6.0: use XML API based configuration templates (see class script.XmlApiConfigTemplate).
tod	TOD - Time Of Day Range Policy.
todsuite	TOD Suite - Time Of Day Suite Policy for Egress and Ingress Entries.
topology	CPAM: Topology - All CPAM topology configurations including BGP, IS-IS, OSPF, CPAA, Links, Routers, Areas, Subnets, Checkpoints, and Route Alarms.
topologysim	CPAM: Simulated Topology - CPAM simulated IGP topology including Links, Routers, Areas, Subnets, and IP Paths.
trapmapper	Trap to Alarm Mapper - Trap to Alarm Mapper.
tunnelmgmt	Tunnel Management - All Tunnel related objects including Hubs, Spokes, Meshes, Chains, Rings, Two Neighbor, Class Forwarding and Rule-based Groups.
udprelay	UDP Relay - UDP Relay configuration and services for layer2.Bridge, DHCP Snooping for VLANs and Ports.
udptunnel	UDP Tunnel - Access to UDP Tunnel.
user	User Preference - NFM-P Client GUI preferences for Info Tables.
vlan	VLAN - Access to this package is for configuring TLS, MVR, Super VLAN, Customer VLAN, SAP and MSAP, Network Interfaces (Uplink Ports) and VLAN configuration for a MST Instance.
vlan.EthernetService	VLAN Ethernet Service - Access to VLAN Ethernet Services.
vlan.L2AccessInterface	VLAN Access Interface - Access to VLAN Access Interfaces.
vlan.Site	VLAN Site - Access to VLAN Sites.
vlan.Vlan	VLAN Service - Access to Virtual LAN (VLAN) Service objects themselves.
vll	VLL - All contained objects are listed. Package access is not currently used.
vll.Endpoint	Endpoint - Access to VLL Endpoints.
vll.L2AccessInterface	L2 Access Interface - Access to VLL L2 Access Interfaces (except Ipipe).
vpls	VPLS - Access to this package is for configuring MLD Snooping, PIM Snooping, DHCP Relay, Multicast CAC Level and LAG Port Down events, and discovered VLAN Elements.
vpls.BL2AccessInterface	VPLS B-L2 Access Interface - Access to VPLS B-L2 Access Interfaces on a VPLS Service.
vpls.BSite	VPLS B-Site - Access to VPLS B-Sites on a VPLS Service.
vpls.Endpoint	VPLS Endpoint - Access to VPLS Endpoints on a VPLS Service.
vpls.EvpnSite	VPLS eVPN-Site - Access to VPLS eVPN-Sites on a VPLS Service.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

Table B-4 Permissions assigned to NFM-P scope of command roles (continued)

Package.Class.Method/Property	Description
vpls.IL2AccessInterface	VPLS I-L2 Access Interface - Access to VPLS I-L2 Access Interfaces on a VPLS Service.
vpls.ISite	VPLS I-Site - Access to VPLS I-Sites on a VPLS Service.
vpls.L2AccessInterface	VPLS L2 Access Interface - Access to VPLS L2 Access Interfaces (except I and B) on a VPLS Service.
vpls.L2ManagementInterface	VPLS L2 Management Interface - Access to VPLS L2 Management Interfaces on a VPLS Service.
vpls.Site	VPLS Site - Access to VPLS Sites (except I and B) on a VPLS Service.
vpls.Vpls	VPLS Service - Access to Virtual Private LAN Service (VPLS) Service objects themselves.
vprn	VPRN - Access to this package is for configuring VPRN Router Instance Sites, SNMP Community, IPsec Interfaces, Group Interfaces, SAPs, MSAPs, IGMP Host Tracking on Sites and SAPs, and FR Interface Specifics for VPRN specific SAPs.
vprn.DVRSSite	VPRN dVRS Site - Access to dVRS VPRN Sites on a VPRN service.
vprn.IPMirrorInterface	IP Mirror Interface - Access to VPRN IP Mirror Interfaces.
vprn.L3AccessInterface	VPRN L3 Access Interface - Access to VPRN L3 Access Interfaces.
vprn.Site	VPRN Site - Access to VPRN Sites.
vprn.SubscriberInterface	VPRN Subscriber Interface - Access to VPRN Subscriber Interfaces.
vprn.Vprn	VPRN Service - Access to Virtual Private Routed Network (VPRN) Service objects themselves.
vprn.VprnPing	VPRN Ping - Access to VPRN Ping tests, VPRN Ping test definitions, and VPRN Ping deployed tests.
vprn.VprnTrace	VPRN Trace - Access to VPRN Trace tests, VPRN Trace test definitions, and VPRN Trace deployed tests.
vrrp	VRRP - Virtual Router Redundancy Protocol (VRRP) configuration on rtr.NetworkInterface, IES and VPRN access interfaces, Authentication Keys, Priority Control Policies and Events.
vs	Scheduler Policy - Scheduler Policies.
webclient	WebClient - Access to the WebClient.
wlangw	WLAN Gateway - WiFi Offload.
workspace	Workspace - Ability to view workspaces, and Create/Edit/Delete private workspaces.
workspace.WorkspaceManager.method_publicControl	Workspace Manager - method_publicControl - Ability to create/edit/delete public workspaces.
wpp	WPP - Web Portal Protocol.
wpp.Site	WPP Site - Access to WPP Sites.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms

B.3 What is the permissions access for NFM-P scope of command roles?

B.3.1 Overview

Each predefined scope of command role has defined access levels to the available permissions based on what the role is designed to do. Permissions grant the following levels of access to an object package, class, method or property:

- Read-only—provides read access to an object class without the ability to create or delete objects.
- Read/write—provides full access to an object class that includes read, create, update/execute, and delete access.
- Read/update/execute—provides read and update/execute access to an object package or property, but does not provide delete access.
- Update/execute—provides update/execute access on class methods, and is typically combined with read access on the parent object package.
- No access.

To view the permission configuration of a scope of command role (default or custom), open the properties form of the role by performing the following steps:

1. Choose Administration→Security→NFM-P User Security from the main menu. The NFM-P User Security manager opens.
2. Click on the Scope of Command tab.
3. Select Role (Security) from the drop-down menu and click Search.
4. Select the required role and click Properties. The Role (Edit) form opens.
5. Click on the Permissions tab.

The Permissions tab lists all permissions and the current access level configured on the scope of command role.

© 2026 Nokia.
Use subject to Terms available at: www.nokia.com/terms